PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

FACULTAD DE INGENIERIA

MAESTRÍA EN REDES DE COMUNICACIONES

TRABAJO PREVIO LA OBTENCION DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACIÓN

TEMA:

"ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA SISTEMAS INFORMÁTICOS – CASO DE ESTUDIO MINISTERIO DE JUSTICIA, DERECHOS HUMANOS Y CULTOS"

LUIS EDUARDO MONTENEGRO FIERRO

Quito, abril 2016

AGRADECIMIENTO

Agradezco a todas las personas que colaboraron en el desarrollo de este proyecto de investigación, en primer lugar a Dios por guiar cada día mi camino, a toda mi familia que siempre me supieron dar ánimos y estuvieron pendientes de mí, al personal administrativo y docente de la Pontificia Universidad Católica del Ecuador y todos quienes con sus palabras de aliento supieron aportar al desarrollo del presente proyecto.

DEDICATORIA

El presente proyecto está dedicado a Dios por cuidar cada día mis pasos y darme la fortaleza y sabiduría para culminar con éxito este proceso académico.

A mis hijos Erick Sebastián e Isabela Valentina por prescindir de su tiempo y recibirme siempre con su alegría, son mi motivación en la vida; los amo.

A mi querida esposa Fernanda quien con su apoyo y compañía son mi soporte para seguirme superando.

A mis padres Luis y Cecilia quienes han sabido guiarme por el buen camino y me han apoyado en mis decisiones.

A mis hermanos Guido, Juan y Kleber que con sus palabras siempre me animaron a seguir y terminar la maestría.

A mis sobrinos Camila, Joel y Mateo que son el mejor regalo que un hermano me pudo dar.

A mis cuñado/as Rocio, Aleja y Christian por su apoyo y preocupación.

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

1 Introducción

Este trabajo presenta, la elaboración de un Plan de Contingencia para Sistemas Informáticos – Caso de Estudio Ministerio de Justicia, Derechos Humanos y Cultos. El fin principal es proporcionar un nivel de disponibilidad continuo de los recursos informáticos de la institución.

Las instituciones públicas y privadas, en este caso el Ministerio de Justicia, Derechos Humanos y Cultos debe estar preparado para solventar cualquier tipo de incidentes, que en el caso de desastres la interrupción prolongada de los servicios informáticos involucraría pérdidas económicas, malestar a los funcionarios y ciudadanía que hacen uso de los recursos mencionados.

Un plan de contingencia en esencia es la capacidad que tiene una institución para recuperarse ante un desastre de la manera más rápida y efectiva; para lo cual se deben ejecutar actividades transparentes para el usuario que permitan minimizar el impacto del incidente en un periodo de tiempo aceptable.

Las repercusiones que involucran la falta de un plan de contingencia o la incorrecta implementación del mismo son fundamentalmente el descontento de los usuarios que genera desconfianza en la institución.

1.1 Planteamiento del Problema

Todas las entidades públicas y privadas deben cumplir normas, requisitos y requerimientos, el Ministerio de Justicia, Derechos Humanos y Cultos al ser una institución pública está sometido a las leyes y normas del estado ecuatoriano. Con el fin de dar cumplimiento a las recomendaciones realizadas por los organismos de control, se encuentra en la necesidad de elaborar un plan de contingencia para los sistemas informáticos.

La Dirección de Tecnologías de la Información y comunicaciones de las instituciones, en este caso el Ministerio de Justicia, Derechos Humanos y Cultos cuentan con algunos mecanismos de control de los sistemas de información los cuales no poseen un estudio adecuado del impacto que permita gestionar de manera formal la prevención y recuperación de desastres; en virtud de lo expuesto se plantea el desarrollo del Plan de Continuidad de los Sistemas Informáticos que están enfocados a brindar el apoyo a todas las gestiones que realizan los funcionarios de la institución.

1.2 Justificación

Una gran parte de instituciones públicas y privadas no cuenta con un plan de contingencia que permitirá solventar los incidentes que pongan en riesgo las operaciones de la institución donde se vean afectados sus sistemas informáticos, en tal virtud se ve en la necesidad de realizar el estudio y

elaboración de un plan de contingencia que pueda ser implantado en instituciones públicas o privadas.

El presente caso de estudio para el Ministerio de Justicia, Derechos Humanos y Cultos presentará una solución bien definida y estructurada que permita mantener operativa las funciones críticas de la institución cuando ocurra una contingencia sobre la infraestructura tecnológica que se posee.

El plan de contingencia propone la aplicación de medidas preventivas y correctivas dentro de los procesos críticos de la institución, los cuales están enfocados a minimizar y reducir el impacto negativo ante la presencia de incidentes o eventos que generen riesgo para el cumplimiento de la misión de la institución.

1.3 Objetivos

1.3.1 Objetivo General.

Desarrollar un Plan de Contingencia para Sistemas Informáticos – caso de estudio Ministerio de Justicia, Derechos Humanos y Cultos.

1.3.2 Objetivos Específicos.

- Evaluar los riesgos de TIC que afecten la continuidad del negocio en las instituciones.
- Gestionar los riesgos que incidan en la generación de eventos críticos.
- Determinar métricas que permitan gestionar los procesos críticos apoyados en las TIC.
- Generar procesos, procedimientos y políticas para mantener la operatividad de los servicios de TIC.
- Determinar responsables para la implementación del plan de continuidad del negocio en la institución.

1.4 Alcance

El alcance del desarrollo del Plan de Contingencia está enfocado a dar cumplimiento a los objetivos específicos planteados en el presente proyecto, donde el área de TIC es la responsable de brindar el soporte tecnológico a los funcionarios de la institución y velar por la seguridad de la información y operación de la infraestructura tecnológica ubicada en el centro de datos de la institución. A continuación se proceden a detallar los objetivos específicos del proyecto:

Evaluar los riesgos de TIC que afecten la continuidad del negocio en las instituciones.

El análisis y evaluación de los riesgos va a ser realizado mediante la implementación de la metodología MAGERIT, se procederá a la aplicación de los pasos de la metodología con el fin de obtener los riesgos a ser tomados en cuenta en el proyecto; dentro de los sistemas informáticos nos centraremos en el análisis de las aplicaciones (sistema de gestión penitenciaria) e infraestructura (servidores, enlaces de datos y equipo de red).

Gestionar los riesgos que incidan en la generación de eventos críticos.

La gestión de riesgos estará delimitada por la implementación de metodologías donde se definen las etapas de la misma; del análisis y evaluación de los riesgos obtenidos se procederá a elaborar los procesos que permitan gestionar los posibles desastres; dentro de los sistemas informáticos nos centraremos en los riesgos para las aplicaciones (sistema de gestión penitenciaria) e infraestructura (servidores, enlaces de datos, equipo de red).

Determinar métricas que permitan gestionar los procesos críticos apoyados en las TIC.

Es importante tener un parámetro que permita cuantificar los niveles de servicio en un plan de continuidad; dentro de este contexto se hará referencia a las métricas de continuidad de los sistemas de información, donde se realizará la implementación de la métrica de tiempo de recuperación RTO y de la métrica de punto de recuperación RPO. De la aplicación de las métricas

se obtendrán valores que ayudaran a determinar el nivel de criticidad de los procesos de la organización asociadas a las TIC en el área aplicaciones (sistema de gestión penitenciaria) e infraestructura (servidores, enlaces de datos, equipo de red).

Generar procesos, procedimientos y políticas para mantener la operatividad de los servicios de TIC.

Se procederá a realizar el diseño del plan de contingencia del negocio donde se detallaran las medidas preventivas, correctivas y las relaciones de coordinación entre las áreas de la institución. Se deberá establecer el formato de cada uno de los procesos y procedimientos a ser aplicados a los eventos de contingencia presentados en el área aplicaciones (sistema de gestión penitenciaria) e infraestructura (servidores, enlaces de datos, equipo de red).

Determinar responsables para la implementación del plan de continuidad del negocio en la institución.

En base al orgánico funcional de la institución se determina cada uno de los responsables de las áreas de la institución que participará en la implementación del plan. Se establecerá un coordinador del Plan de Contingencia y se elaborará un organigrama de responsabilidades y competencias. La máxima autoridad o su delegado será el encargado de designar al responsable de la implementación del Plan de Contingencia en la institución.

1.5 Situación Actual

Se procede a realizar el estudio sobre la metodología para el análisis de riesgos, su aplicación y desarrollo del plan de contingencia que permita mantener la continuidad del negocio para los servicios soportados por las TIC.

1.5.1 Metodologías de Análisis de Riesgos.

Las metodologías para análisis de riesgos tienen como fin de diseñar el Plan de Gestión de Riesgos del sistema, e identificar la aplicabilidad de controles en una organización. Luego de haber identificado y clasificado los riesgos, pasamos a realizar el análisis de los mismos, donde se estudia la posibilidad y las consecuencias de cada factor de riesgo con el fin de establecer el nivel de riesgo de nuestra Organización. El análisis de los riesgos determinará cuáles son los factores de riesgo que potencialmente tendrían un mayor efecto sobre nuestra organización que deben ser gestionados por el personal de la organización (Eterovic & Pagliari , 2011).

En base a la verificación y recomendaciones emitidas por la mayoría de organizaciones y expertos sobre el análisis de gestión de los sistemas de información se hace referencia a la metodología MAGERIT III que está directamente relacionada con la generalización del uso de las tecnologías de la información, y que posee diferentes funcionalidades, variedad de herramientas de gestión que la soportan, se adapta a los estándares y

normativas emitidas y recomendadas en la gestión de riesgos de los sistemas de información (Moliner López, 2005).

1.5.1.1 Descripción de la Metodología.

Magerit es una metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica de España para minimizar los riesgos en la implantación, mantenimiento y uso de las tecnologías de la información y está enfocada principalmente al sector público (Amutio Gómez, Candau, & Mañas, 2012).

El análisis y gestión de riesgos propuesto por MAGERIT III consiste en la aplicación de mecanismos de control que permitan determinar el riesgo e impacto de amenazas en la institución, para lo cual se siguen los siguientes pasos:

- Determinar los activos relevantes para la Organización.
- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

1.5.1.2 Aplicación de la Metodología.

La aplicación de la metodología MAGERIT III permitirá dar cumplimiento en lo establecido por los siguientes estándares internacionales:

- Sistemas de gestión de seguridad de información (ISO 27001)
- Guía para la gestión de seguridad de TI (ISO 13335)
- Análisis de riesgos (ISO 27005)
- Gestión de riesgos (ISO 31000)

Los estándares mencionados tienen como fin realizar la identificación de riesgos, realizar el análisis y evaluación de riesgos y dar el tratamiento adecuado a los riesgos con el fin de reducir su impacto o neutralizarlos definitivamente (Chavez, 2013).

1.5.2 Plan de Contingencia

1.5.2.1 Conceptos.

Sistemas de Información

Un sistema de información es un conjunto estructurado de elementos interrelacionados que tienen como fin proveer la información necesaria para la ejecución de las actividades de una organización, los cuales de acuerdo a su fin o consecución y para objeto de estudio serán categorizados como:

personas, información, procesos, equipos (informáticos y de comunicación) (Rodríguez Sánchez, 2012).

Contingencia

Una contingencia es el cambio de estado de una actividad o tarea en la cual se produce la alteración del cumplimiento de la misma debido a un evento no previsto que genera un impacto negativo en la imagen y servicios que brinda la institución.

Plan de Contingencia

Un plan de contingencia es el conjunto de medidas preventivas y correctivas que permiten mantener operativas las actividades de la institución mediante la implementación de mecanismos que provean las herramientas necesarias que al ser aplicadas en la infraestructura, información y personal técnico de la institución garanticen solventar en el menor tiempo posible los eventos presentados en la infraestructura tecnológica y por ende restablecer la continuidad de las aplicaciones y sistemas informáticos. Para la implementación de un Plan de contingencias Informático es necesario aplicar el ciclo de vida iterativo[1] PDCA[2] (plan-do-check-act) que mediante la retroalimentación de información permite obtener una mejora continua de los procesos de la institución. El ciclo PDCA enseña a las instituciones a planear

[1] Iterativo.- repetición continúa.
[2] PDCA.- ciclo de Deming, (plan-do-check-act), es decir, planificar-hacer-comprobar-actuar; es una estrategia de mejora continua de la calidad para los procesos de la institución.

una acción, hacerla, revisarla para ver cómo se adecua al plan y actuar en base a lo que se ha aprendido.

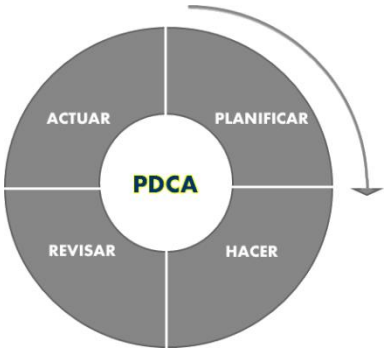


Figura 1. Ciclo de Vida PDCA.

A continuación se procede a describir el ciclo de vida PDCA:

- Planificar.- etapa en la que se establecen las tareas a llevar a cabo para implantar el sistema indicando, definir sus responsables y los plazos.
- Hacer.- etapa donde se lleva a cabo las acciones planificadas anteriormente, entre otras cosas, se incluyen la conformación, la comunicación, la documentación, los procesos, el mantenimiento y difusión de las mismas.
- Revisar.- A esta etapa le corresponde el seguimiento y medición de los controles establecidos en las auditorías internas, así como la implementación de acciones correctivas y preventivas. Una vez implantado el sistema de gestión la auditoría interna nos permite conocer las fallas en nuestro sistema y definir en la siguiente etapa las acciones correctivas necesarias para solventarlas.

- Actuar.- En esta etapa se realiza una evaluación de todo el proceso revisando desde el inicio del ciclo, pasando por todas las etapas y estableciendo las acciones necesarias para mejorarlo, sirviendo como nuevo punto de inicio a la etapa de planear.

La implementación del plan de contingencia para los sistemas informáticos es necesario identificar las amenazas que afectaran los servicios y procesos de la institución, valorar su impacto, categorizarlos, seleccionar las contramedidas (salvaguardas) que serán aplicadas y documentar el plan de contingencias, ya que servirán como referencia para realizar mejoras en los procesos y procedimientos aplicados dentro del ciclo de vida.

1.5.2.2 Metodología de un Plan de Contingencia.

La elaboración del plan de contingencia debe ser guiada por la metodología que permita adaptarse tanto a la infraestructura y servicios que posea y ofrezca la institución; un proyecto de plan de contingencia consiste en realizar:

- Análisis de impacto en el negocio (BIA[3]).- Consiste en identificar los procesos críticos del negocio y los servicios de TIC que los soportan, dimensionar el impacto en los servicios de TIC, nivel

[3] BIA.- análisis del impacto al negocio.- elemento utilizado para estimar el nivel de afectación que podría padecer una organización como resultado de la ocurrencia de algún incidente o un desastre.

de afectación (parcial o total) y definir los requerimientos de recuperación establecidos por la institución, tiempo máximo de interrupción y pérdida de datos máxima permitida.

- Análisis de riesgos.- Consiste en estimar el riesgo potencial al que están sometidos los sistemas de TIC, evaluando el impacto asociado a la materialización de una amenaza, y definir aquellas recomendaciones o controles preventivos que permitan reducir o eliminar dicho riesgo (Ortega, 2011).
- Definición de las estrategias de recuperación.- Consiste en establecer los escenarios de recuperación en función de las amenazas determinadas en el análisis de riesgos y los requerimientos de negocio definidos en el análisis de impacto. En esta fase se define el escenario tecnológico óptimo para soportar los procesos del negocio, atendiendo a las disponibilidades del servicio (Ortega, 2011).
- Desarrollo e implementación del Plan de Contingencia.- Una vez definida la estrategia de recuperación, el plan debe definir y establecer aquellos procedimientos, manuales técnicos y checklists funcionales que permitan restaurar los servicios de TIC(sistemas, operaciones y datos) después de una emergencia o afectación total o parcial de estos servicios. La implementación del plan consiste en la ejecución de las recomendaciones establecidas en el análisis de riesgos y el escenario tecnológico definido (Ortega, 2011).

- Pruebas y mantenimiento del plan.- Las pruebas del plan son esenciales para identificar las deficiencias de planificación y preparación del personal. Además, el plan debe ser un documento que se actualiza periódicamente para mantenerse al día con los cambios en los sistemas de TIC.

Existen algunos aspectos importantes en el modelamiento e implementación del plan de contingencia que son los siguientes:

- Es aconsejable utilizar una herramienta tecnológica que permita realizar el análisis de riesgos. Actualmente existen varias herramientas con sus ventajas y desventajas, a continuación algunas: PILAR, Meycor, Proteus, Ecija (PCN, SGSI), etc (Ortega, 2011).
- Es necesario definir los procesos de continuidad y disponibilidad de TIC que permitan mantener actualizado el plan frente a cambios de infraestructura y/o servicios de TIC (Ortega, 2011).
- Definir los criterios de activación del plan, ya que el plan debería activarse cuando la evaluación de los daños indique que los criterios han sobrepasado el lumbral máximo permitido.
- Las actividades de recuperación definen el escenario tecnológico adecuado que cumpla con los requerimientos de continuidad del negocio; esto puede conllevar una inversión económica considerable la cual es necesaria analizarla cuidadosamente.

1.5.3 Continuidad del Negocio y las TIC.

La continuidad del negocio describe los procesos y procedimientos que la institución debe ejecutar para garantizar que los procesos y servicios estén operativos durante y después de un desastre.

La función del plan de continuidad del negocio es evitar la indisponibilidad de los procesos y servicios críticos de la institución y restablecerlos de forma rápida y efectiva.

Misión Crítica

Misión crítica se refiere a la infraestructura, operaciones y servicios que son absolutamente necesarias para que una institución lleve a cabo su misión; para cada institución el significado de misión crítica puede ser diferente ya que será definido de acuerdo a las necesidades de la misma. Por ejemplo cada institución determinará qué elementos de su infraestructura y servicios de red de TIC son de misión crítica. Esto incluye dispositivos como: switches, routers, plataformas de servicios, dispositivos de seguridad, aplicaciones, medios de almacenamiento y medios de transmisión.

Los recursos de misión crítica son necesarios para que los procesos y servicios lleven a cabo su tarea; en el caso de que cualquiera de estos elementos falle debido a un mal dimensionamiento, diseño, factores ambientales, defectos físicos o errores de los funcionarios se deberán aplicar las contramedidas elaboradas para que las operaciones.

Características de la Infraestructura de Misión Crítica

Se recomienda que una institución posea las siguientes características en su plataforma de misión crítica:

- Simplicidad y Redundancia.- Una infraestructura modular con el menor número de componentes es recomendable porque facilitan su manejo y reemplazo. La redundancia podría afectar esta característica porque aumenta el número de componentes, pero dará mayor fiabilidad en el funcionamiento.
- Costo.- El costo es un factor importante al momento de elegir un producto o servicio, este tiene que ser analizado en base a los objetivos, estrategias de disponibilidad y mejoramiento de desempeño en las aplicaciones y servicios que la institución necesita.
- Capacidad de Servicio.- Consiste en solventar de manera adecuada todos los requerimientos solicitados, en caso de ser necesario soportar cierto porcentaje de crecimiento o demanda de servicios sin degradar su rendimiento.
- Reemplazo y mantenimiento de dispositivos.- Este término hace referencia a la rapidez con la que los componentes o dispositivos son reemplazados y detectados dentro de un sistema, sin tener que reiniciarlo.
- Tolerancia a Fallos.- Es la capacidad que tienen los sistemas para seguir operando en caso de que ocurra un incidente y

afecte alguno de sus componentes (Alegsa, Definición de Tolerancia de fallas, 2010).

- Garantía y cobertura.- Los equipos tecnológicos deben poseer soporte del fabricante los cuales garanticen el cumplimiento de estándares y normas en su funcionamiento.
- Funcionalidad.- La plataforma debe satisfacer las necesidades de la institución.
- Plataforma.- La plataforma base de trabajo también conocida como sistema operativo debe ser seleccionada de acuerdo a los requerimientos necesarios para que las aplicaciones y servicios sean soportados de manera adecuada; este puede ser licenciado o de distribución libre.

1.5.3.1 Alta disponibilidad en aplicaciones e infraestructura.

La alta disponibilidad es la característica que tiene un sistema o solución para protegerse y recuperarse de interrupciones o caídas de sus servicios por ende su infraestructura de forma automática y en un corto plazo.

Los sistemas y plataformas en alta disponibilidad están diseñadas para soportar los fallos ocasionados por eventos imprevistos, la forma más adecuada para este fin es aplicar la redundancia en sus componentes (red, almacenamiento, fuentes de alimentación, etc.) así como de los elementos de infraestructura (sistema eléctrico, aire acondicionado, electrónica de red, etc.)

y aplicaciones. Las aplicaciones dispuestas en alta disponibilidad permiten realizar balanceo de carga y distribución de la data (bases de datos) evitando problemas de saturación y tiempos de respuesta alto en periodos de tiempo cuando la concurrencia es alta (Gorenberg, 2006).

Tolerancia a Errores

Es la propiedad que permite a un sistema continuar operando adecuadamente en caso de una falla en alguno de sus componentes (Alegsa, Definición de Tolerancia de fallas, 2010). La tolerancia a errores es indispensable en aquellos sistemas y servicios que deben estar activos todo el tiempo; al ocurrir una falla en un dispositivo o componente otro componente tomará el control de sus tareas para subsanar o minimizar los efectos del fallo. Una forma de lograr tolerancia de fallas, es duplicar cada componente del sistema.

Un sistema o servicio consiste en un conjunto de componentes de hardware y software que son diseñados para proveer un servicio específico, donde un desperfecto en un sistema ocurre cuando no desempeña sus actividades de la manera especificada (Ramirez, 2016).

Un fallo es una condición anormal de funcionamiento las cuales pueden ser ocasionadas por: errores de diseño, problemas de fabricación, deterioro por el uso u otros problemas externos (como condiciones ambientales

adversas, interferencia electromagnética, entradas imprevistas o el mal uso del sistema).

Las plataformas con tolerancia a fallos tienen como fin solventar los fallos generados en uno o varios de sus componentes, permitiéndole trabajar dependiendo del caso con restricciones pero sin parar los servicios. A continuación algunos de los criterios necesarios de una plataforma con tolerancia a fallos:

- Identificar inmediatamente los errores o fallos.
- Seguir proporcionando el servicio al ocurrir un fallo.
- Corregir el problema.
- Mantener el estado de los trabajos y operaciones.
- Reanudar las operaciones sin causar errores ni problemas en sus servicios y aplicaciones.

Existen algunas alternativas que nos permiten proporcionar tolerancia a fallos para los servicios de TIC dentro de una institución:

- Hardware y Software.
- Redundancia de componentes.
- Verificación de errores mediante alertas.
- Mecanismo de recuperación automática.

Redundancia de Componentes

La redundancia implica, necesariamente, duplicar infraestructura. Quizás es la forma más tradicional de implementar un modelo de redundancia es a través de los modelos de clusterización, en los cuales mediante algún protocolo de conmutación dos equipos que funcionan coordinadamente se alternan de acuerdo a parámetros pre-definidos en caso de una fallar uno de los dos (Marcos, Redundancia, Contingencia, Continuidad, Resiliencia, 2011). Los esquemas en este caso pueden ser Activo – Pasivo (sólo uno funciona en el tiempo), o Activo – Activo (cuando ambos funcionan simultáneamente, debe existir algún mecanismo adicional que realice balanceo de carga) (Marcos, Redundancia, Contingencia, Continuidad, Resiliencia , 2011). Por ejemplo, los esquemas de firewall con redundancia, pueden requerir switches y routers duplicados, además de los firewalls, y en algunos casos incluso será necesario duplicar enlaces físicos para obtener una solución completa.

En la práctica, la estrategia preferida por las instituciones es ubicar los esquemas de redundancia en Data Centers, esto hace que encontremos soluciones con disponibilidad real del 99.6%. Se debe tener en cuenta que el implementar una infraestructura redundante involucra un alto costo económico ya que como se indicó anteriormente se debe duplicar la plataforma tecnológica de la institución.

1.5.3.2 Estructura de la plataforma tecnológica.

Las instituciones tienen como finalidad proveer de manera continua la prestación de servicios a sus clientes, en tal virtud se debe tener en cuenta la plataforma tecnológica base con la que se pueda brindar un servicio con alta disponibilidad. A continuación se procede a detallar los equipos recomendados que deberán contar con redundancia:

REDUNDANCIA EN EQUIPOS TECNOLOGICOS

SERVIDORES

Los equipos servidores que alojan las aplicaciones y servicios críticos de la institución deben poseer componentes redundantes, a continuación se procede a indicar los componentes del servidor a ser redundantes:

- CPU.- Es necesario que el servidor posea por lo menos 2 cpu físicos con varios núcleos, esta característica permitirá seguir operando hasta reemplazar el dispositivo.
- Discos Duros.- Es necesario que el servidor por lo menos cuente dos discos duros que permitan el almacenamiento de la información. La característica que permite a los discos duros brindar alta disponibilidad es RAID[4] donde su principal valor es el poder seguir trabajando aunque se dañe algún disco duro, adicionalmente el servidor debe poseer la característica de

[4] RAID.- Arreglo Redundante de Discos, combina múltiples discos duros en un arreglo, y almacena la información procurando evitar que se pierdan datos si uno o más discos llegan a fallar.

hotswap (cambio en caliente) que permite reemplazar un disco duro cuando el servidor se encuentre encendido.

- Memorias.- El servidor debe poseer los suficientes bancos para instalar memorias RAM.
- Interfaces de Red.- Se debe poseer dos interfaces de red las mismas que el momento que sea necesario entre en funcionamiento (modo activo-pasivo, modo activo-activo)y por ende el servicio se mantenga arriba.
- Fuentes de Poder.- Es necesario que el servidor posea por lo menos 2 fuentes de poder redundantes hotswap que permitan seguir operando en caso de una falle, estas fuentes deberán ser alimentadas desde circuitos eléctricos diferentes como puede ser servicio eléctrico convencional y planta de energía .
- Ventiladores.- de igual manera deben existir al menos 2 ventiladores hotswap que permitan trabajar temporalmente al equipo.
- Suministro Eléctrico.- Se recomienda poseer una fuente de alimentación eléctrica regulada con respaldo de energía, así como de una planta generadora que proporcionará la energía necesaria para que la infraestructura tecnológica funcione.

Es necesario realizar un balanceo de carga entre servidores con el fin de mantener la alta disponibilidad y evitar saturar el procesamiento de

peticiones concurrentes a cada una de las aplicaciones o servicios alojados en el equipo por parte de los clientes.

Con el fin de mantener un mejor control y manejo de los recursos de cada uno de los servidores se introduce el concepto de clúster que es la unificación de los recursos de cada uno de los servidores los que serán tratados como un todo (pool de recursos), la característica principal es que las aplicaciones o servicios seguirán funcionando aunque se detecte algún fallo físico en algún recurso de los servidores. Esta tecnología es aplicada en ambientes virtualizados donde se realiza la asignación de recursos de manera dinámica y de acuerdo a la demanda del servicio o aplicación. La configuración de una infraestructura de clúster permite manejar solicitudes concurrentes a servicios y aplicaciones, tolerancia a fallos, balanceo de carga, alta disponibilidad, etc.

EQUIPOS DE RED

La infraestructura de red permite la comunicación tanto de los equipos servidores así como de los usuarios dentro y fuera de la institución; por tal motivo se recomienda mantener redundancia en los equipos de comunicación, a continuación se procede a describir los equipos recomendados:

- Router.- dispositivo que permite la interconexión de varios segmentos de red tanto desde la red interna como desde y hacia la red externa.

- Switch.- dispositivo de red encargado de la interconexión de varios segmentos de red que son asignados a los usuarios dentro de la institución.
- Patch Cords.- medio de comunicación que permite conectar diferentes tipos de dispositivos, actualmente de cobre o fibra óptica.
- Enlaces.- por lo general los enlaces permiten el acceso ya sea a internet o enlaces entre sitios, este servicio es proporcionado por el proveedor ISP.

Seguido de la anterior descripción de equipos que componen una red, se procede a mostrar un esquema de conexión de red redundante:

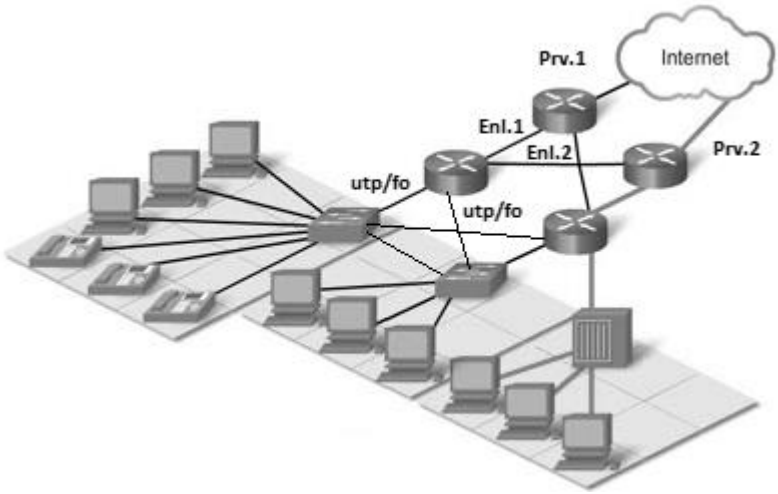


Figura 2. Redundancia componentes de red.

Para obtener esta estructura de red redundante es necesario realizar las respectivas configuraciones de alta disponibilidad en cada uno de los componentes de red.

ESTRUCTURA DE RED

Es necesario aplicar ciertos criterios de diseño (tamaño, ubicación, escalabilidad, etc.) que permitan adaptar la estructura de la red a las necesidades de la institución. A continuación se procede a mencionar los criterios de diseño de una red:

SEGMENTACION

Un diseño segmentado es la mejor práctica para una red de misión crítica. La arquitectura segmentada involucra separar una red en zonas, o módulos. Un módulo es el más bajo nivel de funcionamiento independiente, pudiendo ser un único componente hasta un segmento de red. El diseño segmentado reduce el riesgo de caída de servicios, al limitar el impacto de un problema a un módulo o grupo de módulos, a veces llamado grupo de fallo. De esta manera un evento adverso en un grupo no afecte la operación de toda la red.

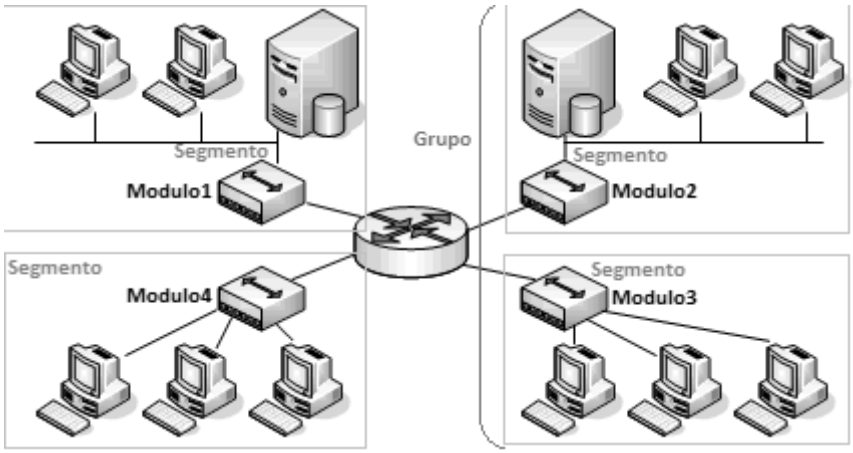


Figura 3. Estructura de red segmentada.

BALANCEO DE CARGA

Consiste en proporcionar una estructura de red que independientemente de su disposición (centralizada, descentralizada) tenga los suficientes recursos para solventar los requerimientos de los equipos finales.

Arquitectura Centralizada.- La centralización es un diseño que consolida los recursos de la red en una sola ubicación (nodos, plataforma, o centro de datos), permite reducir el costo y la complejidad de instalación, administración y mantenimiento. Ofrece un uso más eficiente de los recursos y reduce los costos operativos; dicha consolidación conlleva a una menor flexibilidad y mayor riesgo de indisponibilidad de los servicios o recursos de la institución.

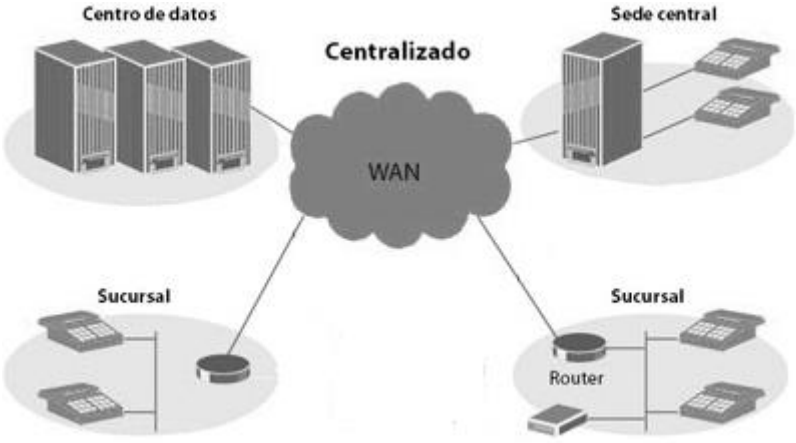


Figura 4. Arquitectura de red centralizada.

Arquitectura Descentralizada.- Consiste en la separación y replicación de servicios y aplicaciones en distintos equipos y sitios diferentes. La implementación de arquitecturas distribuidas o descentralizadas implica el uso

de más equipos y dispositivos lo que conlleva a mayores gastos operacionales. Los sistemas descentralizados ofrecen una mayor flexibilidad con la posibilidad de utilizar diferentes proveedores, equipos y servicios.

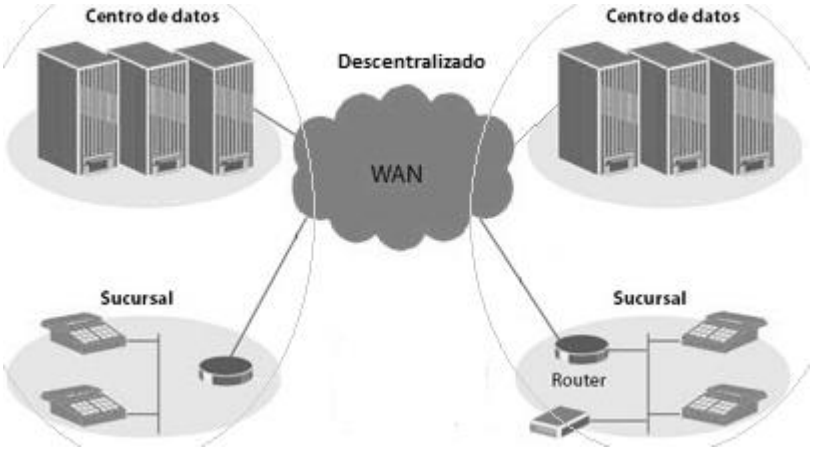


Figura 5. Arquitectura de red descentralizada.

ESCALABILIDAD

La arquitectura de red escalable presenta la posibilidad de que en caso de ser necesario se pueda agregar una cantidad de dispositivos de red sin afectar el rendimiento y disponibilidad de los servicios y aplicaciones (LAURA, 2009). Escalabilidad es la capacidad que posee nuestro sistema para soportar mayor cantidad de trabajo donde estas sean razonables en términos de costo, tiempo y complejidad.

La escalabilidad en una red es una medida del número de usuarios finales o los nodos de usuarios atendidos por una red. El alcance de una red es el número de usuarios finales y la ubicación de los nodos de los usuarios a los que presta servicios. La escalabilidad supone un factor crítico en el

crecimiento de una red, si una red tiene como objetivo crecer en el número de usuarios manteniendo su rendimiento actual (MADEJA, 2013), tiene que evaluar dos posibles opciones:

- Con un hardware de mayor potencia o
- Con una mejor combinación de hardware y software.

Se pueden distinguir dos tipos de escalabilidad, vertical y horizontal:

- Escalamiento vertical.- significa el añadir más recursos a un solo nodo en particular dentro de un sistema, tal como el añadir una tarjeta de expansión a un switch.
- Escalamiento horizontal.- significa agregar más nodos a un sistema, tal como añadir una computadora, impresora o dispositivo de red a un área de la institución.

Figura 6. Escalabilidad de la red.

1.5.3.3 Métricas aplicadas para la continuidad del negocio.

Una métrica es un medio para controlar, predecir y probar el correcto desempeño de un servicio o aplicación. Las métricas son aplicadas con el

propósito de evaluar la calidad del servicio. Con el fin de determinar el correcto funcionamiento de un servicio o aplicación es necesario definir indicadores que no son más que el conjunto de métricas que permiten cuantificar un servicio.

METRICAS DE RECUPERACION

Con el fin de mantener la continuidad del negocio se establece un esquema que ayuda a la institución a recuperarse después de un desastre; un plan de continuidad del negocio, es un mapa que detalla cómo una institución puede continuar operando mientras dura la recuperación del desastre (revista datacenter, 2013). Para lo cual se hace referencia a las métricas de recuperación RPO y RTO.

RTO TIEMPO DE RECUPERACION OBJETIVO

Es el tiempo en el que el proceso del negocio debe estar restaurado después de un incidente grave, con el fin de evitar consecuencias inaceptables derivados de una para en la continuidad del negocio (Cruz, 2015). Para reducir el RTO, se requiere que la Infraestructura (tecnológica, logística o física) esté disponible en el menor tiempo posible pasado el evento de interrupción. RTO define el límite de tiempo máximo tolerable para recuperar los datos si se produce un desastre y los sistemas esten disponibles inmediatamente. Ejemplo: cuando no existe pérdida de datos el RTO es cero; pero si se tolera una hora para recuperación de datos, el RTO es una hora.

RPO PUNTO DE RECUPERACION OBJETIVO

RPO es la edad (tiempo que tiene un respaldo) de los archivos que se deben recuperar de almacenamiento de copia de seguridad para las operaciones tras un incidente grave; el RPO se expresa desde el instante en que el incidente se produce, puede ser especificado en segundos, minutos, horas o días; por lo tanto es la cantidad máxima aceptable de pérdida de los datos medidos en el tiempo. Para reducir un RPO es necesario aumentar el sincronismo de réplica de datos. El RPO determina la pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación (Sánchez, 2013).

ANALISIS RPO vs RTO

RPO es específicamente el tiempo máximo establecido entre una copia de seguridad y otra con el fin de mantener la continuidad de los servicios. RPO es esencial para determinar la frecuencia con la que una empresa debe programar copias de seguridad de datos. RTO es el tiempo que tomará una organización para volver a funcionar de acuerdo a los niveles de servicio acordados con sus clientes (sean internos o externos). Ambos son elementos de recuperación de desastres y de la gestión de la continuidad del negocio. Uno de ellos es acerca de cuánto es el tiempo máximo de los datos que van a ser restaurados mientras que el otro se trata del tiempo máximo que llevará reanudar las operaciones (revista datacenter, 2013). Por ejemplo una INSTITUCIÓN podría tener un RPO de 1 semana, pero un RTO de 1 solo día.

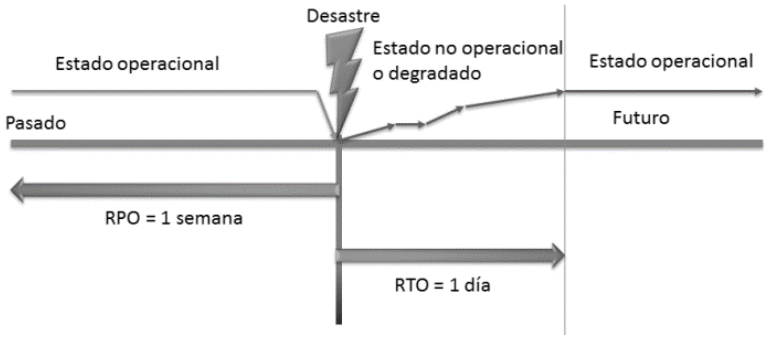


Figura 7. RTO vs RPO. Fuente:https://revistadatacenter.wordpress.com/2013/12/12/cual-es-la-diferencia-entre-el-rto-y-rpo/

A continuación se presenta un breve ejemplo de una contingencia para la recuperación de un desastre con un servidor que contiene una aplicación y bases de datos.

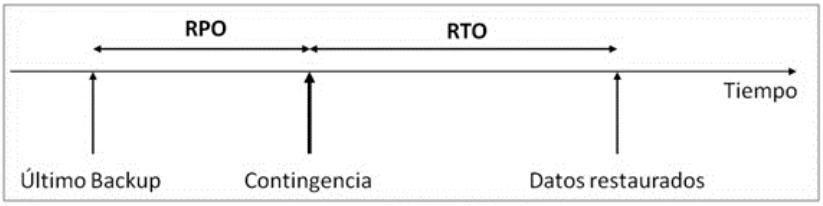


Figura 8. Tiempo de recuperación desastre. Fuente: http://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo

Pasos a seguir para recuperar las aplicaciones y los datos en caso de contingencia:

- Restaurar el servidor (dependiendo del tipo de problema pueden ser minutos, horas o días).
- Restaurar las copias de seguridad, último backup.
- Reanudar la operación del servidor y sistemas alojados

A partir de este punto se deberán repetir los procesos que faltan, desde el momento de la caída hasta el momento de la recuperación, que serán más cuanto mayor sean RPO y RTO (Karman, 2004).

COSTO DE LA RECUPERACION DE DESASTRES

Con el fin de reducir los costos de disponibilidad de servicios del RTO y RPO es necesario disponer de una buena infraestructura y personal adecuado que permita solventar los desastres de manera rápida y oportuna; esto conlleva a una mayor inversión económica que dependiendo de la institución se la podrá realizar o no.

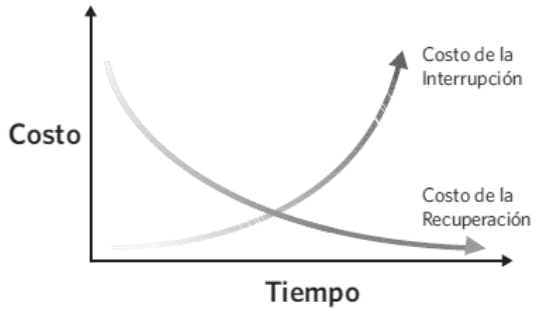


Figura 9. Costo-Recuperación, Costo-Inversión. Fuente: http://www.iss.com.co/soluciones/rm2/dr2

Costo de la interrupción.- Se refiere a que mientras mayor cantidad de tiempo se encuentre caído un sistema más costosas serán las consecuencias e impacto para la institución.

Costo de la recuperación.- Es el costo de los mecanismos de recuperación a implementar, que dependiendo de la inversión el tiempo de recuperación será mayor o menor.

La intercepción de estas dos curvas sería para la institución la inversión adecuada en sistemas de Recuperación de Desastres frente a lo que la institución está dispuesta a aceptar o considera razonable en cuanto a la caída de sus servicios.

METRICAS DE COSTOS

Finalmente con el fin de cuantificar efectivamente los costos que involucran un desastre es necesario establecer las métricas de costos que ayudaran a evaluar el impacto y la inversión económica justa y necesaria a realizar en la institución. Los costos en caso de un desastre o durante la inactividad en una institución involucran un valor no necesariamente económico que perjudica a la imagen de la institución desde el momento que ocurre el mismo hasta que finaliza el incidente. Los costos involucran la cantidad de recursos ya sean económicos, físicos o humanos que serían necesarios para solventar un incidente de la mejor manera y en el menor tiempo posible. Se debe tomar en cuenta que cualquier tipo de degradación o disminución de tiempo de respuesta en un servicio o aplicación por debajo de los límites aceptables involucra un incidente que está provocando un costo para la institución; se debe poner mucho más énfasis en los periodos de inactividad que conllevan en generar costos de inactividad que dependiendo de la razón de ser de la institución pueden involucrar repercusiones económicas, sociales y humanas afectando de manera muy negativa a la institución. Los costos por inactividad están asociados a tres tipos que son los siguientes:

Costos Directos.- Se llama costo directo, al conjunto de las partidas presupuestarias en las que incurre cualquier institución, sin importar el fin, que están directamente relacionados a la obtención del producto o servicio en torno al cual gira la institución. Son aquellos que pueden identificarse

directamente con un objeto de costo, los costos directos se derivan de la existencia de aquello cuyo costo se trata de determinar, sea un producto, un servicio, una actividad, como por ejemplo, los materiales directos y la mano de obra directa destinados a la fabricación de un producto, o los gastos de propiedad intelectual por parte de los técnicos para presentar un servicio (Horngren, Datar, & Rajan, 2012).

Costos Indirectos.- Son aquellos que intervienen en el proceso de generación de un producto o servicio; “Son aquellos costos cuya identificación con un objeto de costos específico es muy difícil, o no vale la pena realizarla. Para asignar los costos indirectos a los distintos departamentos, productos o actividades, es necesario, normalmente, recurrir a algún tipo de mecanismo de asignación, distribución o reparto. Los costos comunes a varios productos, servicios, o costos conjuntos, reciben también el tratamiento de costos indirectos” (contabilidad.com.py, 2006).

Costos Intangibles.- La mayoría de los costos intangibles se sitúan en la categoría de costos de fallos externos, como por ejemplo la pérdida de imagen de la institución. No obstante también pueden aparecer cuando la empresa incurre en fallos internos, por ejemplo la desmotivación de los empleados. “Son Difíciles de estimar y podrían ser desconocidos; estos incluyen perder una ventaja competitiva, perder la reputación por no ser el primero con una innovación o un líder en un campo, deterioro de la imagen de la institución debido al incremento en la insatisfacción del cliente y toma de

decisiones ineficaz debido a la información inoportuna o inaccesible. Como puede imaginar es casi imposible proyectar con precisión una cantidad en dólares para los costos intangibles. Sirven para ayudar a tomar decisiones en el proceso de evaluar el sistema propuesto y todas sus implicaciones, se deben incluir los costos intangibles aunque no sean cuantificables" (Osmer, 2013).

2 Análisis y Evaluación de Riesgos

El análisis y evaluación de riesgos es la etapa en la que se recopila la información sobre las causas de las posibles amenazas, los daños y consecuencias sobre la infraestructura tecnológica que éstas puedan producir en las operaciones de la institución, esto con el fin de tomar decisiones y administrar los riesgos de forma apropiada.

Los resultados del análisis de riesgos permitirán disponer de información suficiente para proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades reales de la institución.

2.1 Análisis de Riesgos

La realización del análisis de riesgos proporciona a las instituciones una visión de la situación en cuanto al nivel de protección de los sistemas de información. Por este motivo, se constituye como uno de los pilares fundamentales a la hora de conocer de manera detallada la infraestructura y

el funcionamiento interno de los procesos. A continuación se proceden a indicar las tareas que se deben realizar en el análisis de riesgos:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de perjuicio (costo) que supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza (Amutio Gómez, Candau, & Mañas, MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas, 2012).

2.1.1 Identificación de Activos

Busca identificar los activos[5] de información de la institución, para ello se debe establecer qué es y qué no es un activo de información. La tipificación de activos debe además contemplar unificar como un activo a todos aquellos

[5] Activo.- Es un objeto o recurso de valor empleado en una empresa u organización.

recursos que tengan características comunes y que la información que administran, procesan o almacenan tenga el mismo grado de criticidad, confidencialidad y disponibilidad. Deben agruparse aquellos recursos a los que se les puede aplicar la misma estrategia de seguridad. En esta fase se obtiene el inventario de activos de información (Revista ALIDE, 2013).

2.1.1.1 Objetivos.

Identificar los activos que componen la infraestructura de TI para los servicios de la institución, determinado sus características, atributos y clasificación.

2.1.1.2 Productos y Servicios.

Con el fin de recopilar la información necesaria para el proyecto es necesario realizar o poseer los siguientes documentos que servirán como producto base en la elaboración del plan de contingencia:

- Inventario de Datos
- Inventario de Equipos Servidores
- Inventario de Software
- Inventario de Equipos de comunicación
- Diagrama de estructura de Red

Adicionalmente es necesario clasificar los activos con el fin de agrupar y gestionarlos de manera más adecuada y eficiente, se lo realizará de acuerdo a la siguiente clasificación:

ACTIVOS ESENCIALES

Tabla 1
Activos esenciales

Activos Esenciales	
Información	Abarcan requisitos de seguridad para todos los demás componentes del sistema
Personal	nivel bajo
Clasificación	nivel confidencial
Servicio	Información
Activos	Actas
	Terminos de Referencia
	Contratos con proveedores
	Manuales de configuraciones
	Licencias
	Plan estrategico informático

Activos Esenciales	
Información	Abarcan requisitos de seguridad para todos los demás componentes del sistema
Personal	nivel medio
Clasificación	difusión limitada
Servicio	Servicios
Activos	Sistemas de acceso solo personal institución
	Sistemas de acceso público
	Sistemas interinstitucionales

Datos

- Servicios Auxiliares.- dispositivos que ayudan indirectamente al funcionamiento de la institución.
- Documentación y Registros.- Consiste en mantener un archivo donde se almacene la documentación de la institución que esté

involucrada con la infraestructura y servicios contratados y adquiridos.

Tabla 2
Activos datos

Activos Datos	
Tipo	Activos auxiliares
Descripción	Otros elementos que ayudan al funcionamiento de la institución
Activos	Suministros de oficina

Activos Datos	
Tipo	Documentación y registros
Descripción	Información no electrónica que contiene datos
Activos	Reglamentos de la empresa
	Informes de consultorias
	Manuales de sistemas y usuarios
	Oficios
	Memorandos
	Contratos
	Actas

Servicios

- Comunicaciones.- servicios contratados por la institución con un proveedor de servicios.
- Energía.- Proveedor del servicio eléctrico.
- Cloud.- Servicios que se posee en un proveedor de cloud, donde se encuentran montados algunas aplicaciones.

Tabla 3
Activos servicios

Activos Servicios	
Tipo	Comunicaciones
Descripción	Servicios y equipos de comunicación provistos por un ISP
Activos	Datos
	Internet
	Telefonía

Activos Servicios	
Tipo	Suministro de energía eléctrica
Descripción	Servicios y medios de transmisión de energía eléctrica
Activos	Acometida red eléctrica
	ups
	planta generadora

Activos Servicios	
Tipo	Correo electrónico
Descripción	Dispositivo que permite el envío y recepción de documentos electrónicos mediante el acceso a su aplicación, previo a la validación de credenciales de acceso
Activos	Front end (interfaz de conexión para los usuarios)
	mailbox (almacenamiento de datos)

Aplicaciones Informáticas

- Sistemas Operativos.- Consiste en registrar todos los diferentes sistemas operativos que estén instalados sobre los equipos servidores y de escritorio de la institución.
- Paquetes software.- constituyen los programas y/o aplicaciones genéricas que permiten la ejecución de tareas a los funcionarios y que están instaladas en los equipos de la institución.
- Aplicaciones.- software que fue creado en base a un requerimiento especifico de la institución y que sirve como plataforma de gestión para los servicios de la institución.

Tabla 4
Activos aplicaciones informáticas

Activos Aplicaciones Informáticas	
Tipo	Sistemas operativos
Descripción	Un sistema operativo es el conjunto de programas informáticos que permite la administración eficaz de los recursos de una computadora.
Activos	Windows server 2003
	Windows server 2008 r2
	Linux centos 5.5
	Linux centos 6.0
	Linux centos 7.0
	Windows xp
	Windows 7

Activos Aplicaciones Informáticas	
Tipo	Programas y software estandar
Descripción	software genérico, que resuelve múltiples necesidades, y la empresa probablemente sólo empleará algunas. En general, es un software que no se adapta completamente al vocabulario, necesidades y funciones que necesita la empresa.
Activos	libreoffice
	office
	openfire
	navegadores
	mysql
	antivirus
	mensajeria

Activos Aplicaciones Informáticas	
Tipo	Software a la medida
Descripción	El software a la medida es aquél sistema que se diseña y desarrollo de manera personalizada y única. Es decir, busca complacer todas las necesidades y adaptarse lo mejor posible a lo que una empresa necesita
Activos	aplicaciones gestión departamentales
	correo electrónico
	portales web
	aplicaciones publicadas al público
	Repositorios documentales
	Software de inteligencia de negocios
	Gestión de procesos

Activos Físicos

Los activos físicos constituyen todos los equipos tecnológicos con los que cuenta la institución, a continuación se presentan los principales:

- Equipos Portátiles.- constituyen los equipos portátiles los cuales pueden ser trasladados de un lugar a otro.
- Equipos de Escritorio.- Son los equipos que se encuentran en cada una de las dependencias de la institución.
- Equipos Oficina.- equipos adicionales de tecnología que ayudan en la ejecución de las tareas diarias de los funcionarios.
- Equipos Servidores.- equipos que alojan las respectivas aplicaciones y servicios de la institución.

- Equipos de Comunicación.- equipos que permiten interconectar cada uno de los elementos de la red.
- Enlaces de Comunicación.- medios físicos por los cuales se transmite la información de la institución.

Tabla 5
Activos equipos informáticos

Activos Equipos informáticos	
Tipo	Equipos portatiles
Descripción	Equipos que pueden ser transportados de un lugar a otro
Activos	Computadoras portatiles
	modems

Activos Equipos informáticos	
Tipo	Equipos escritorio
Descripción	Equipos que se encuentran instalados en un lugar fijo de la institución
Activos	Compuatdoras de escritorio

Activos Equipos informáticos	
Tipo	Equipos oficina
Descripción	Equipos que permiten el envio y recepción de información
Activos	Impresoras
	Telefonos
	Fax
	Scanners

Activos Equipos informáticos	
Tipo	Equipos servidores
Descripción	Equipos que permiten la administración, almacenamiento y gestión de la información, aplicaciones y servicios de la institución
Activos	Servidor de correo
	Servidor de controlador de dominio
	Servidor de aplicaciones
	Servidor Web
	Servidor de base de datos
	Servidor antivirus

Activos Redes de comunicaciones	
Tipo	Medios de comunicación
Descripción	Medios que proveen la comunicación en la institución, generalmente son cableados o inalambricos.
Activos	Acometida internet, datos
	cableado estructurado
	patch cords cobre, fibra optica
	Inalambricas

Activos Instalaciones	
Tipo	Edificios
Descripción	Lugares físicos donde se alojan los funcionarios y equipos tecnologicos de la institución
Activos	Edificio planta central
	Edificio delegaciones provincias

2.1.1.3 Recurso Humano.

Personas

Se refiere al personal quien es el o los encargados de administrar las aplicaciones y recursos tecnológicos de la institución.

Tabla 6
Activos personas

Activos Personas	
Tipo	Personal
Descripción	Funcionarios en general de la institución y el personal técnico de TI
Activos	Técnicos unidad de TIC

2.1.2 Dependencia entre Activos.

Las dependencias entre activos permiten relacionarse con los demás activos con datos y servicios. Se podría decir que se formaría un árbol de dependencias; consiste en determinar los activos que dependen uno (activo padre) de otro (activo hijo) y su grado de impacto en el caso de un incidente. Las dependencias se usan para propagar el valor (es decir, los requisitos de seguridad) desde los activos valiosos (arriba) a los activos que soportan el valor por delegación (abajo). Con el fin de determinar la relación de dependencia entre los activos se deben elaborar los diagramas de dependencias de activos.

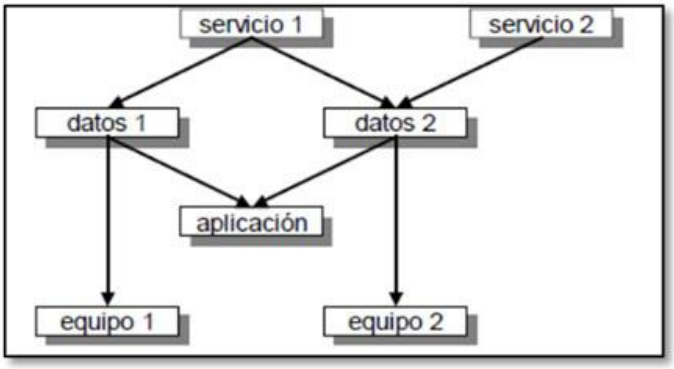


Figura 10. Diagrama dependencia entre activos (superiores e inferiores).
Fuente:http://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/

Adicionalmente se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

Activos Esenciales

- Información que se maneja dentro de la institución
- servicios prestados a los funcionarios y a la ciudadanía
- Servicios Internos
- Que se estructuran ordenadamente el sistema de información
- El equipamiento informático
- Aplicaciones (software)
- Equipos informáticos (hardware)
- Comunicaciones (enlaces)
- Soportes de información: discos, cintas, etc.

El entorno: activos que se precisan para garantizar las siguientes capas

- Equipamiento y suministros: energía, climatización, etc.
- Mobiliario

Los servicios subcontratados a terceros

Las instalaciones físicas

El personal

- Usuarios
- operadores y administradores
- desarrolladores, técnicos (Amutio Gómez, Candau, & Mañas, 2012)

2.1.3 Valoración de Activos.

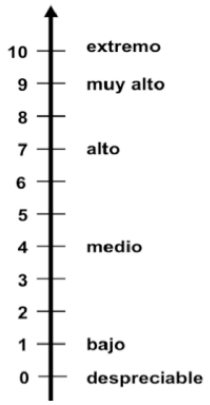
Una vez identificados todos los activos, el siguiente paso es valorarlos. Se refiere al valor que se asigne a cada activo de acuerdo al grado de importancia, además siempre resguardando la disponibilidad, integridad, confiabilidad y disponibilidad de cada uno de ellos. La valoración de un activo puede ser cuantitativa (numérica 0 a 10) o cualitativa (niveles nivel bajo, nivel medio, nivel alto). “La valoración se puede ver desde la perspectiva de la necesidad de proteger pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes” (Amutio Gómez, Candau, & Mañas, 2012).

Adicionalmente se debe determinar las escalas o niveles de recuperación de incidentes para los activos en cuestiones de disponibilidad; aquí se establecen los tiempos de respuesta que pueden tener los activos, a continuación se presenta un ejemplo:

- 45m.- se dispone de 45 minutos para solventar incidentes críticos sobre activos críticos.
- 60m.- tiempo de respuesta para solventar incidentes sobre activos de prioridad media.
- 90m.- tiempo de respuesta para solventar incidentes sobre sistemas críticos pero el impacto es medio.
- 120m.- tiempo de respuesta para solventar incidentes sobre sistemas de prioridad media e impacto medio.
- 1 día.- tiempo de respuesta para solventar incidentes sobre activos de prioridad baja donde existe un impacto de nivel bajo.

2.1.3.1 Escalas de valoración.

Son la asignación de valores ya se cuantitativos o cualitativos a un incidente ocurrido sobre los activos de la institución. Frecuentemente la valoración es cualitativa, quedando a discreción del usuario; es decir, respondiendo a criterios subjetivos. “Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). Si se realiza un análisis de riesgos de poco detalle, se puede optar por la tabla simplificada de menos niveles. Ambas escalas, detallada y simplificada se correlacionan como se indica a continuación” (Amutio Gómez, Candau, & Mañas, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos, 2012).



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Figura 11. Criterios de valoración de activos. Fuente: (Amutio Gómez, Candau, & Mañas, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos, 2012)

2.1.3.2 Resultados de la valoración.

El resultado de la valoración de un activo debe ser enfocado a la disponibilidad de un servicio o aplicación; donde una hora de para de servicios es irrelevante, mientras que un día sin servicio causaría un daño significativo, pero un mes significa el fin de la actividad de la institución. En conclusión no existe proporcionalidad entre el tiempo de interrupción y las consecuencias de este.

Para valorar la interrupción de la disponibilidad de un activo hay que usar una estructura más compleja que se puede resumir en un gráfico como el siguiente:

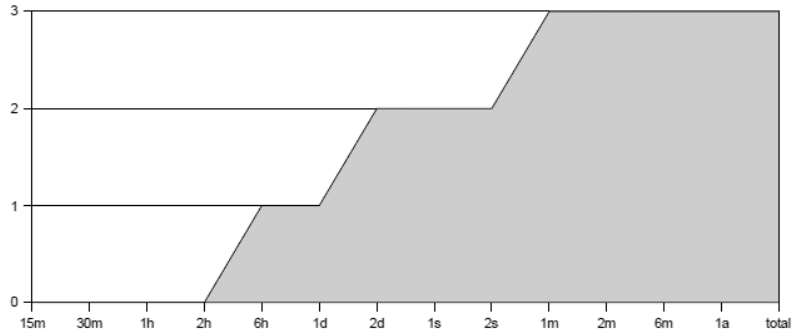


Figura 12. Costo de la interrupción de la disponibilidad.
Fuente:http://cursos.aiu.edu/AN%C3%81LISIS%20DE%20RIESGOS%20EN%20SISTEMAS/Sesi%C3%B3n%202/PDF/metodo%20de%20analisis%20de%20riesgos%201.pdf

Aparece una serie de niveles de interrupción que terminan con la destrucción total o permanente del activo (Amutio Gómez, Candau, & Mañas, MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas, 2012). En el ejemplo anterior, paras de hasta 6 horas se pueden asumir sin consecuencias. Pero a las 6 horas se disparan las alarmas que aumentan si la para supera los 2 días. Y si la para supera el mes, se puede decir que la Organización ha perdido su capacidad de operar. Desde el punto de vista objetivo la gráfica dice que no hay que gastarse ni un centavo por evitar paras de menos de 6 horas. Vale la pena un cierto gasto por impedir que una para supere las 6 horas o los 2 días. Y cuando se valore lo que cuesta impedir que la para supera el mes, hay que poner en la balanza todo el valor de la Organización frente al costo de las salvaguardas.

Para la valoración de los activos de la institución se estableció la dimensión disponibilidad para la estimación del riesgo que podría afectar a los

activos. A continuación se procede a mostrar el análisis implementado en los procesos de la institución:

Tabla 7
Valoración de procesos del negocio de la institución

Categoría Activos	Activo	Valoración Magerit	Valoración institución
Procesos del Negocio	Servicios	3	5
	Nomina	3	5
	Bienes	3	5
	Compras Públicas	7	6
	Contabilidad	3	5
	Jurídico	3	5
	Auditoria interna	1	4
	Atención ciudadanía	5	5
	Rehabilitación Social	4	6
	Asuntos interinstitucionales	5	5

Los resultados del análisis mostrado en la tabla 7 nos indican que estos son los procesos críticos de la institución los mismos que nos servirán como base para la implementación del plan de contingencia. A continuación se procede a valorar los servicios y aplicaciones informáticas que soportan cada uno de los procesos.

Tabla 8
Valoración de los servicios de la institución

Categoría Activos	Activo	Valoración Magerit	Valoración institución
Servicios	Internet	3	2
	Intranet	3	2
	Comunicaciones lan/wan	5	2
	Portales web	3	3
	Correo electrónico	4	3
	Soporte técnico	5	2

Como se indicó anteriormente se aplicó la dimensión disponibilidad para la valoración de los servicios de la tabla 8 que están enfocados para satisfacer las necesidades de los funcionarios de la institución como a la ciudadanía. A continuación se procede a valorar las aplicaciones informáticas

de la institución que sirven como plataforma para la gestión de los procesos y servicios críticos de la institución.

Tabla 9
Valoración de los sistemas y aplicaciones de la institución

Categoría Activos	Activo	Valoración Magerit	Valoración institución
Sistemas/Aplicaciones	Sistema Talento Humano	3	3
	Sistema Financiero	5	2
	Sistema Planificación	3	3
	Sistema Gestión Penitenciaria	7	1
	Sistema videoconferencias	3	3
	Sistema Gestión de Bienes	3	3
	Sistema de Gestión Documental	4	3
	Correo Electrónico	4	3
	Portal Web	3	3

Luego de haber analizado los activos de servicios y aplicaciones es necesario realizar la valoración de la infraestructura que permite la prestación de los mismos.

Tabla 10
Valoración de equipos Servidores y de Comunicación (red)

Categoría Activos	Activo	Valoración Magerit	Valoración institución
Equipos Servidores y de Comunicación	HP BL460C G6 Servidor de Correo	5	1
	HP BL460C G6 Servidor de Dominio	5	1
	HP BL460C G6 Servidor de Aplicaciones	5	1
	HP BL460C G6 Servidor Gestión Documental	5	1
	HP BL460C G6 Servidor Web	5	1
	HP BL460C G6 Servidor Antivirus	5	1
	HP DL380 G5 Servidor Base Datos	5	1
	HP DL380 G5 Servidor telefonía IP	5	1
	HP Switch 5406zl Switch Core	5	1
	HP Switch 2910 Switch Distribución/Acceso	3	3
	HP S3020F ngfw Firewall	5	1

La valoración de los activos que cumplen funciones críticas dentro de la institución define la importancia de los mismos, esto quiere decir que al existir un incidente provocaran un gran impacto en la prestación de servicios para la institución.

2.2 Identificación de Amenazas

Consiste en identificar las amenazas[6] que pueden afectar a los activos, son eventos que pueden ocurrir y determinar que daño pueden causarle a nuestros activos.

2.2.1 Tipos de Amenazas.

A continuación se procede a indicar el catálogo de amenazas propuesto por la metodología Magerit III que pueden afectar a los activos de un sistema de información (Amutio Gómez, Candau, & Mañas, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos, 2012):

De origen natural

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[6] Amenazas.- Causa potencial de un incidente que puede causar daños a un sistema de información o una organización.

Origen: Natural (accidental).- Hay accidentes naturales (terremotos, inundaciones, etc). Ante estas alteraciones el sistema de información es víctima pasiva, pero de todas formas se debe tener en cuenta lo que puede suceder con los activos de información de la institución.

Tabla 11
Amenazas de origen natural

Tipo	Clasificación
[N] DESASTRES NATURALES	[N.1] Fuego
	[N.2] Daños por Agua
	[N.*] Desastres Naturales

Del entorno (de origen industrial)

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada. Hay desastres industriales (contaminación, fallos eléctricos, etc.) ante los cuales el sistema de información es víctima pasiva.

Tabla 12
Amenazas del entorno (de origen industrial)

Tipo	Clasificación
[I]ORIGEN INDUSTRIAL	[I.1] Fuego
	[I.2] Daños por Agua
	[I.*] Desastres Industriales
	[I.3] Contaminación mecánica
	[I.4] Contaminación Electromagnética
	[I.5] Averia de origen fisico o lógico
	[I.6] corte del suministro eléctrico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[I.8] Fallo de servicios de comunicaciones
	[I.9] Interrupción de otros servicios o suministros esenciales
	[I.10] Degradación de los soportes de almacenamiento de información
	[I.11] Emanaciones Electromagéticas

Defectos de las aplicaciones

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades[7].

Causadas por las personas de forma accidental

Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

Origen: Humano (accidental)

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

[7] Vulnerabilidades.- Defectos de fábrica que suelen afectar a los sistemas de software.

Tabla 13
Amenazas defectos de las aplicaciones

Tipo	Clasificación
[E] ERRORES Y FALLOS NO INTENCIONADOS	[E.1] Errores de los Usuarios
	[E.2] Errores del Administrador
	[E.3] Errores de Monitorización (log)
	[E.4] Errores de Configuración
	[E.7] Deficiencias en la Organización
	[E.8] Difusión de Software Danino
	[E.9] Errores de [re-]encaminamiento
	[E.10] Errores de Secuencia
	[E.14] Escapes de información
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de la información
	[E.19] Fugas de Información
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[E.25] Pérdida de equipos
	[E.28] Indisponibilidad del personal

Causadas por las personas de forma deliberada

Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

Origen: Humano (deliberado)

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de

beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

Tabla 14
Amenazas causadas por personas de manera intencional

Tipo	Clasificación
[A] ATAQUES INTENSIONADOS	[A.3] Manipulación de los registros de actividad (log)
	[A.4] Manipulación de la configuración
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.8] Difusión de software dañino
	[A.9] [Re-]encaminamiento de mensajes
	[A.10] Alteración de secuencia
	[A.11] Acceso no autorizado
	[A.12] Análisis de tráfico
	[A.13] Repudio
	[A.14] Interceptación de información (escucha)
	[A.15] Modificación deliberada de la información
	[A.18] Destrucción de información
	[A.19] Divulgación de información
	[A.22] Manipulación de programas
	[A.23] Manipulación de los equipos
	[A.24] Denegación de servicio
	[A.25] Robo
	[A.26] Ataque destructivo
	[A.27] Ocupación enemiga
	[A.28] Indisponibilidad del personal
	[A.29] Extorsión
	[A.30] Ingeniería social (picaresca)

2.2.2 Valoración de Amenazas en Aplicaciones e Infraestructura.

La valoración de amenazas está enfocada a determinar la frecuencia con la cual se pueden presentar las amenazas y dimensionar el daño que tendrá un activo si esta llegara a ocurrir. Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el

valor del activo, esto se lo hace en tomando en cuenta los siguientes parámetros:

- Degradación.- consiste en estimar en qué nivel se perjudica el activo. La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción" (Amutio Gómez, Candau, & Mañas, 2012).
- Probabilidad.- consiste en determinar cuán probable o improbable es que se materialice una amenaza. La probabilidad de que ocurra un evento sobre un activo por lo general será realizada mediante escala cualitativa.

Cuando las amenazas no son intencionales, únicamente bastará conocer la fracción física perjudicada de un activo para calcular la pérdida proporcional del activo; cuando la amenaza es intencional no se calcula la proporción del daño ya que el efecto del ataque estará direccionado directamente a un servicio o equipo (Amutio Gómez, Candau, & Mañas, 2012).

Tabla 15
Degradación del valor

ITEM	CATEGORIA	DESCRIPCION	NIVEL
MA	MUY ALTA	casi seguro	fácil
A	ALTA	muy alto	medio
M	MEDIA	posible	dificil
B	BAJA	poco probable	muy dificil
MB	MUY BAJA	muy raro	extremadamente dificil

Recuperado de (Amutio Gómez, Candau, & Mañas, 2012)

Generalmente se modela numéricamente como una frecuencia de ocurrencia; habitualmente se usa 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia[8] como medida de la probabilidad de que algo ocurra (Amutio Gómez, Candau, & Mañas, 2012). A continuación algunos valores típicos:

Tabla 16
Probabilidad de ocurrencia

ITEM	VALORES	DESCRIPCION	FRECUENCIA
MA	10	muy frecuente	a diario
A	100	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Recuperado de (Amutio Gómez, Candau, & Mañas, 2012)

La degradación en un activo dimensiona el daño causado por un incidente en el caso de que este ocurriera. Se caracteriza con una fracción del valor del activo.

Tabla 17
Escala de degradación

Nivel	Degradación
25%	Poco
50%	Medio
75%	Alto
100%	Muy Alto

Finalmente se procede a realizar la valoración de amenazas de la institución de acuerdo a las siguientes categorías:

- Amenazas para el tipo de activo Hardware

[8] Ocurrencia.- idea, acción inesperada y repentina.

- Amenazas para el tipo de activo Software
- Amenazas para el tipo de activo Datos
- Amenazas para el tipo de activo Servicios

Amenazas activo HARDWARE

Tabla 18
Amenaza activo hardware

Amenaza(clasificación)	Degradación (%)	Frecuencia	Análisis
Fuego (N.1-I.1)	25%	MUY BAJA	El centro de datos de la institución posee un sistema de detección y control de incendios. Los cuartos de equipos del edificio donde se encuentran equipos de comunicación solo cuentan con extintores. Existen personas responsables de la administración y supervisión de los sistemas de incendios, los cuales son monitoreados mediante un sistema que envía notificaciones vía email y SMS al detectar un incidente. Es indispensable mantener el servicio de garantía y mantenimiento del sistema de incendios, se lo debe realizar por lo menos 2 veces al año
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Desastres Naturales(N.*)	25%	MUY BAJA	El centro de datos de la institución se encuentra ubicado en un lugar estratégico (libre de tuberías y acometidas de agua) de la institución, lo cual permite evitar desastres como inundaciones si las hubiere. Adicionalmente no se han registrado contingencias en casos de fenómenos naturales como terremotos, derrumbos, etc. La contingencia en caso de un desastre natural seria poseer un sitio alterno en otro lugar distante geográficamente, este puede ser nacional o internacional
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**

Desastres Industriales: energía eléctrica(I.*)	50%	MEDIA	Las variaciones de voltaje son bastante comunes en las instituciones, lo cual produce una degradación en el funcionamiento de los equipos del 60%. LA variación o interrupción del suministro de energía produciría un grave daño en los equipos donde la información se podría perder. La centro de datos de la institución posee una alimentación eléctrica regulada que provee de energía controlada evitando las variaciones de voltaje La institución posee una planta de energía que entra en funcionamiento al perder la alimentación de energía pública Es necesario contratar el mantenimiento de los equipos de energía y planta eléctrica, realizarlo por lo menos 2 veces al año
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Avería de origen físico o lógico en los equipos (I.5)	50%	MEDIA	Es importante realizar el monitoreo de los componentes de los equipos mediante herramientas de software que envíen notificaciones vía email o SMS a los responsables de la infraestructura del centro de datos. El fallo en uno de los componentes puede ocasionar la para de servicios y hasta la perdida de información
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Condiciones inadecuadas de temperatura o humedad(I.7)	25%	BAJA	El centro de datos posee un sistema de climatización de precisión, el mismo que es monitoreado y administrado por los responsables. Se posee un sistema de envió de notificaciones vía email y SMS en caso de presentarse incidentes. Adicionalmente se posee un aire acondicionado de respaldo que entra a funcionar en caso de que el principal falle, finalmente se posee un servicio de mantenimiento que se lo realiza 3 veces al año.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: errores del	25%	BAJA	Se dan equivocaciones de manera involuntaria por lo rutinarias de las acciones.

administrador, errores de configuración(E.2-E.4)			No están establecidos los procedimientos de instalación y configuración de los equipos servidores Se debe elaborar un checklist donde se indiquen los procedimientos, responsables y parámetros de configuración de los equipos
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: errores de Mantenimiento/Actualización de equipos(hardware)(E.23)	50%	MEDIA	La institución posee un registro de los equipos del centro de datos donde se indica la versión de su firmware y la fecha de actualización Es necesario mantener el servicio de garantía y mantenimiento de los equipos informáticos, donde el partner será el encargado de realizar la actualización y mantenimiento de los mismos. No se tiene implementada la política donde se indique que para realizar la actualización del firmware primero se deba valorar la compatibilidad con los sistemas operativos y aplicaciones que alberga el equipo. La institución cuenta con diagrama actualizado de red, así como definición de redes, subredes y vlans que permiten la conectividad de los equipos de la institución.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: Caída del sistema por agotamiento de recursos(E.24)	50%	MEDIA	Esta amenaza implica que las aplicaciones dejen de funcionar por la falta de recursos de los componentes de los equipos, virus, etc. El impacto sería el mal funcionamiento de las aplicaciones o la indisponibilidad de los mismos. La institución definió un responsable encargado de realizar el monitoreo y control de recursos de los equipos; adicionalmente el responsable es el encargado de definir y coordinar los mantenimientos y gestión de nuevos recursos para los equipos en caso de necesitarlos.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**

Ataques Intencionados: Manipulación de la configuración, Acceso no autorizado(A.4-A11)	25%	BAJA	La institución tiene montado un sistema de control de acceso al centro de datos que consiste en un usuario y clave, adicionalmente se posee un sistema de monitoreo que es administrado por un responsable y se envían notificaciones vía email y SMS. El acceso a los equipos servidores como de comunicación se lo realiza mediante credenciales unificadas locales. Se tienen implementadas vlans que limitan el acceso de los usuarios o intrusos a la vlan de servicios. Se posee una herramienta de monitoreo de red que es la encargada de censar la conectividad y posibles errores de los equipos.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Ataques Intencionados: Ataque destructivo(A.26)	25%	MUY BAJA	El centro de datos así como todas las instalaciones de la institución es custodiado las 24 horas por personal de seguridad.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Ataques Intencionados: Robo(A.25)	25%	MUY BAJA	No se han registrado robos en la institución, cada equipo es asignado a una persona como custodio y es responsable del mismo. Se firman actas de entrega recepción de bienes. La institución realiza el aseguramiento (póliza de seguro) de equipos críticos así como de los equipos portátiles. La institución posee un circuito cerrado de televisión CCTV, que monitorea y graba permanentemente las áreas críticas (ingresos, egresos, centro de datos, despacho, parqueadero, bodega, etc.) de la institución.

Amenazas activo SOFTWARE

Tabla 19
Amenaza activo software

Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**

Errores y fallos no intencionados: errores de los usuarios(E.1)	50%	MEDIA	Consiste en el desconocimiento del funcionamiento de aplicaciones de la institución, así como el ingreso incorrecto de información. Es necesario definir un proceso de inducción y capacitación sobre el manejo de las aplicaciones al ingreso del personal; adicionalmente se deben manejar acuerdos de confidencialidad de la información cuando lo amerite.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: errores del administrador(E.2)	50%	MEDIA	Se presentan o son causados por el personal técnico que administra los equipos. Al ejecutar procedimientos de instalación, configuración o actualización no se lleva un control o registro del proceso a realizar, causando de esta manera un mal funcionamiento en el equipo que alberga las aplicaciones y servicios de la institución.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: errores de configuración(E.4)	50%	MEDIA	Se define responsables de cada uno de los equipos del centro de datos, así como de las aplicaciones. Es necesario levantar los procesos para la configuración de los equipos y aplicaciones así como de las políticas que permitan seguir funcionando en caso de un incidente, ya que estos fallos pueden afectar de manera significativa a las actividades de la institución.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: difusión de software dañino(E.8)	75%	ALTA	Los virus, troyanos, gusanos, etc. Son amenazas que pueden degradar el rendimiento de las aplicaciones de la institución. Los mecanismos o formas de difusión son principalmente el internet y medios de almacenamiento extraíbles, en tal virtud se deben tener instalados y actualizados los antivirus para mitigar estas amenazas. La institución cuenta con una plataforma base (sistema operativo) donde corren las aplicaciones que son poco vulnerable a este tipo de amenazas.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**

Errores y fallos no intencionados: Escapes de información(E.14)	25%	MUY BAJA	Amenaza que es consecuencia de otro tipo de amenaza como: accesos no autorizados, errores de configuración, aplicaciones vulnerables, manipulación de las configuraciones de los equipos.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: Vulnerabilidad de los programas(software)(E.20)	50%	MEDIA	Es necesario realizar las respectivas pruebas de control de calidad al momento de implementar un nuevo software o módulo de uno ya existente. Los desarrolladores son los responsables del acceso tanto al código fuente y base de datos, por lo tanto deben tomar las respectivas medidas para evitar el acceso no autorizado a los mismos.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: Errores de mantenimiento/actualización de programas(software)(E.21)	50%	MEDIA	Se debe realizar el monitoreo y control del desempeño de las aplicaciones, esto se suele hacer mediante sus logs, de esta manera se puede identificar los errores y fallos en su funcionamiento. Al realizar actualizaciones o implementar nuevas versiones es necesario validarlo en un ambiente de pruebas que se cerciore sobre el correcto funcionamiento.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Ataques intencionados: Manipulación de la configuración(A.4)	50%	MEDIA	Amenaza que es consecuencia de otro tipo de amenaza como: errores de administrador, errores de configuración, difusión de virus, vulnerabilidad de aplicaciones.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Ataques intencionados: Suplantación de identidad del usuario(A.5)	25%	BAJA	Amenaza que es consecuencia de otro tipo de amenaza como: errores de administrador, errores de configuración, difusión de virus, vulnerabilidad de aplicaciones, accesos no autorizados, sesiones abiertas. Se debe implementar una política donde se defina la asignación de claves, reseteo de claves y reasignación de claves y de privilegios de acceso.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**

Ataques intencionados: Uso no previsto(A.7)	25%	BAJA	Los equipos de la institución deben ser usados únicamente para generar productos, información de la institución. No se permite la instalación de software o aplicaciones que no sean necesarias para las labores del personal de la institución, restricción de privilegios.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Ataques intencionados: Manipulación de programas(A.22)	25%	MUY BAJA	Amenaza que vulnera la confidencialidad de la información. Se poseen mecanismos de control de acceso a los equipos servidores, aplicaciones, bases de datos e información que es de carácter confidencial.

Amenazas activo DATOS

Tabla 20

Amenaza activo datos

Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: Errores de los usuarios(E.1)	50%	MEDIA	Equivocaciones que se producen en forma rutinaria de carácter involuntario; pone en riesgo la consistencia de la información de la base de datos de las aplicaciones. Esta amenaza es la consecuencia en fallos que se producen en las aplicaciones.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: Alteración accidental de la información(E.15)	50%	MEDIA	Es consecuencia de amenazas como: errores de configuración, accesos no autorizados, abuso de privilegios, vulnerabilidad de aplicaciones, errores de usuarios. Los ambientes más susceptibles serían los accesos web e intranet.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Errores y fallos no intencionados: Destrucción de la información(E.18)	25%	BAJA	Esta amenaza se presenta como consecuencia de la amenaza

Amenazas activo SERVICIOS

Tabla 21
Amenaza activo servicios

Amenaza(clasificación)	Degradación (%)	Frecuencia	Análisis
Ataques intencionados: Denegación de servicio(A.24)	50%	MEDIA	Es necesario tomar en cuenta la concurrencia de usuarios a las aplicaciones, ya que esto podría ocasionar la indisponibilidad del servicio. Se debe implementar mecanismos de balanceo de carga, firewall y alta disponibilidad en la infraestructura que alberga las aplicaciones de la institución.
Amenaza(clasificación)	**Degradación (%)**	**Frecuencia**	**Análisis**
Ataques intencionados: Indisponibilidad del personal(E.28,A.28)	25%	BAJA	Existen responsables en cada una de las áreas críticas (infraestructura, redes, aplicaciones y soporte técnico) de los servicios y plataforma tecnológica de la institución.

Árbol de Amenazas

A continuación se procede a mostrar el árbol de amenazas al que están expuestos los servicios e infraestructura de la institución:

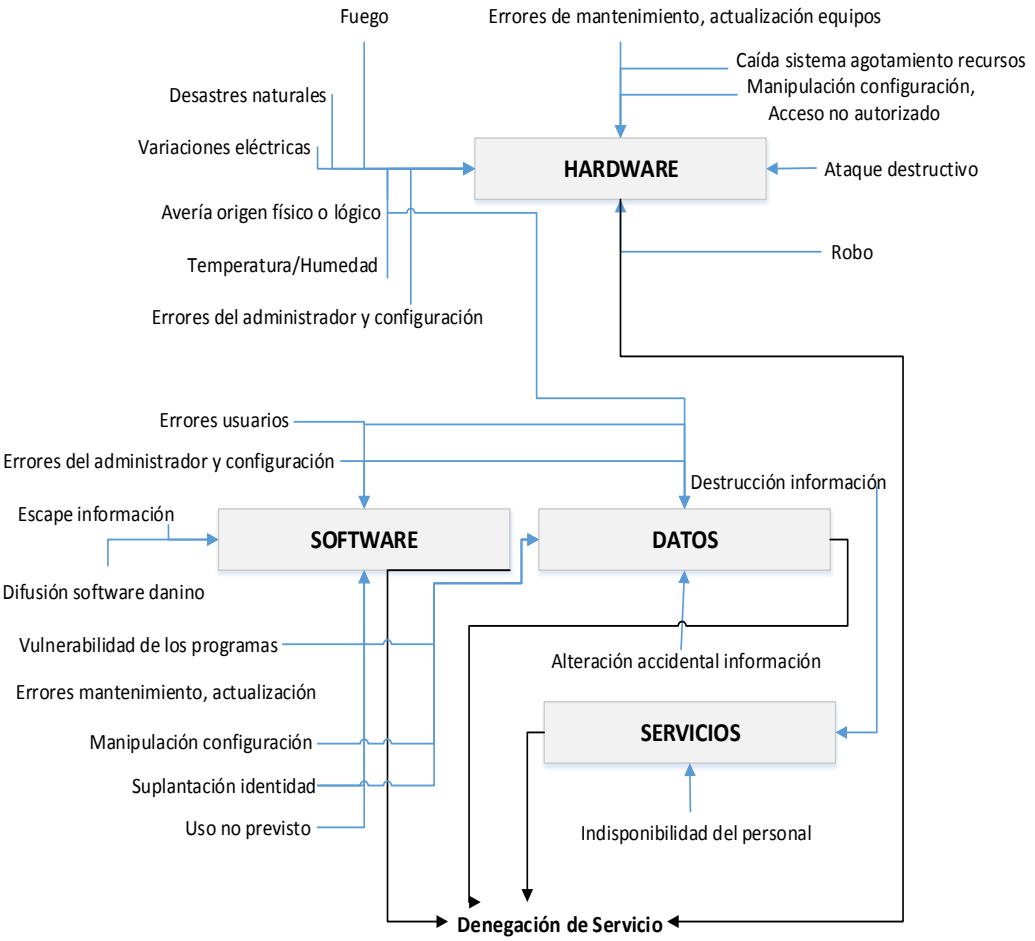


Figura 13. Árbol de amenaza.

2.3 Identificación de Protecciones/Seguridades

Se definen a las protecciones/seguridades como salvaguardas o contra medidas a aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se evitan simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos),

seguridades físicas y mediante la implantación de políticas al personal de la institución. Con el fin de implementar las salvaguardas más adecuadas que se apeguen a la realidad y necesidades de la institución es necesario tomar en cuenta los siguientes aspectos:

- Tipo de activos a proteger, pues cada tipo se protege de una forma específica.
- Dimensión o dimensiones de seguridad que requieren protección.
- Amenazas de las que necesitamos protegernos.
- Si existen salvaguardas alternativas (Amutio Gómez, Candau, & Mañas, 2012).

Finalmente del análisis anterior se concluye que activos deben ser tomados en cuenta para la aplicación de salvaguardas obteniendo así la declaración de aplicabilidad, este proceso debe ser justificado de dos formas:

- No Aplica.- una salvaguarda se aplica porque técnicamente no es adecuada para el tipo de activos a proteger, no protege la dimensión necesaria o no protege cuando se presente la amenaza.
- No se Justifica.- una salvaguarda no se justifica cuando la salvaguarda si aplica pero no en la medida que se necesita proteger.

Las salvaguardas intervienen en el cálculo del riesgo de la siguiente manera:

- Reduciendo la probabilidad de las amenazas.- conocidas como salvaguardas preventivas, ya que llegan a impedir completamente que la amenaza se materialice.
- Limitando el daño causado.- hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para evitar que la degradación avance.

Las salvaguardas ofrecen diferentes tipos de protección a los activos, a continuación se proceden a describirlas:

[PR] Prevención.- una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Ejemplos: autorización de usuarios, gestión de privilegios, metodología desarrollo de software, pruebas en preproducción, segregación de tareas.

[DR] Disuasión.- una salvaguarda es disuasiva cuando tiene un efecto sobre los atacantes que estos no ataquen, actúan antes del incidente reduciendo las probabilidades de que ocurra; si sucede no tienen influencia sobre los daños causados. Ejemplos: señalética, guardias de seguridad, avisos confidencialidad accesos no autorizados.

[EL] Eliminación.- una salvaguarda elimina un incidente cuando impide que se ejecute, actúan antes de que el incidente se haya producido. No

reducen los daños en caso de que el incidente llegue a ocurrir. Ejemplos: eliminación de cuentas sin contraseña, de servicios innecesarios.

[IM] Minimización del impacto / limitación del impacto.- una salvaguarda minimiza o limita el impacto cuando reduce las consecuencias de un incidente.

Ejemplos: desconexión de redes o equipos en caso de ataque, parar servicios en caso de ataque, seguros de cobertura.

[CR] Corrección.- una salvaguarda es correctiva cuando si se ha producido un daño lo repara; actúan después de que el incidente se haya producido. Ejemplos: gestión de incidentes, enlaces de comunicación backup, fuentes de alimentación redundantes, aire acondicionado backup.

[RC] Recuperación.- una salvaguarda ofrece recuperación cuando permite al activo regresar a un estado anterior, reducen las probabilidades del incidente y cuantifican los daños a un periodo de tiempo. Ejemplos: copias de seguridad (backup).

[MN] Monitorización.- monitorean lo que está ocurriendo y lo que ha ocurrido, los incidentes detectados en tiempo real son intervenidos inmediatamente para limitar el impacto; si se detectan eventos luego de ocurridos servirán como antecedente para evitarlos a futuro. Ejemplos: registros de actividad, registro de descargas de web, logs de navegación, logs aplicaciones.

[DC] Detección.- consiste en detectar un incidente e informa de que el ataque está ocurriendo, no impide el ataque pero permite que entren en operación medidas que eviten la progresión del ataque minimizando los daños. Ejemplos: anti-virus, IDS, detectores de incendio.

[AW] Concienciación.- actividades de capacitación a las personas que influyen sobre el sistema. La capacitación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez potenciando su efecto. Ejemplos: cursos de concienciación, capacitaciones.

[AD] Administración.- están relacionadas con los componentes de seguridad del sistema. Una correcta administración evita accesos no autorizados y un correcto funcionamiento de las aplicaciones. Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad.

La siguiente tabla relaciona cada uno de estos tipos de protección con el modelo de reducción de la degradación y de la probabilidad:

Tabla 22
Tipos de salvaguardas

Efecto	Tipo
Preventivas: reducen la provabilidad	[PR] preventivas
	[DR] disuasorias
	[EL] eliminatorias
Acortan la degradación	[IM] minimizadoras
	[CR] correctivas
	[RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización
	[DC] de detección
	[AW] de concienciación
	[AD] administrativas

2.3.1 Análisis de Seguridades existentes en la institución.

Las salvaguardas deberán ser lo más efectivas posibles frente a un riesgo, en tal virtud una salvaguarda ideal sería 100% eficaz al mitigar totalmente una amenaza; técnicamente se combinan 2 factores que garantiza su efectividad:

- Es técnicamente idónea para enfrentarse al riesgo que protege.
- Se emplea siempre.

La eficacia de la salvaguarda desde el punto de vista operativo combina los siguientes factores:

- Está perfectamente desplegada, configurada y mantenida.
- Existen procedimientos claros de uso normal y en caso de incidencias.
- Los usuarios están formados y concienciados.
- Existen controles que avisan de posibles fallos.

Se define una eficacia del 0% para aquellas que faltan o no existen y el 100% para aquellas que son idóneas y que están perfectamente implantadas, para medir los aspectos organizativos, se puede emplear una escala de cumplimiento que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda (Amutio Gómez, Candau, & Mañas, 2012):

Tabla 23
Eficacia y cumplimiento de las salvaguardas

Factor	Nivel	Significado	Descripción
0%	0	inexistente	no se ejecuta
20%	1	inicial	ejecución de manera esporádica, cierto personal
40%	2	reproducible pero intuitivo	se ejecuta informalmente
60%	3	proceso definido	documentado se ejecuta formalmente
80%	4	gestionable y medible	se obtiene indicadores
100%	5	optimizado	se producen mejoras

2.3.2 Valoración de Seguridades.

SALVAGUARDAS IDENTIFICADAS PARA EL TIPO DE ACTIVO HARDWARE

Tabla 24
Salvaguardas activo hardware

Control	Descripción del control / salvaguarda	Amenazas mitigadas
Inventario de Activos	Cuantificar hardware	Robo
	Descripción del hardware	
	Ubicación del hardware	
	Centro de datos	
	Mantenimiento Hardware	
	Asignación uso de hardware	
	Responsable hardware	

Responsable de los activos	Los activos están a cargo de un funcionario que es el responsable.	
Control de acceso a las instalaciones de la institución	El acceso a las instalaciones de la institución están controlados por entidad de seguridad privada	
	El acceso de personas ajenas a la institución es validado por el personal de recepción de la institución, donde se solicita un documento de identidad el cual es devuelto a su salida.	
Ubicación y control de Activos	La ubicación de los activos está registrada en archivo	
	Estado del activo (hardware y software)	
	Hoja de ruta de mantenimiento, preparación de equipos	
Adquisición de equipos	Procesos de evaluación para el dimensionamiento y selección del hardware	Agotamiento de recursos
	Acceso a los recursos del equipo	Manipulación de la configuración
	Uso del equipo	
	Accesos al equipo	
Gestión de cambios (actualización hardware)	Requerimientos hardware	Fallos o averías de origen físico o lógico
	Justificación actualización hardware	
	Impacto hardware adicional	
	Documentación cambios	
Gestión de cambios (reemplazo hardware)	Análisis cambio hardware	
	Impacto reemplazo hardware	
Soporte servicios públicos	Planta generadora eléctrica	
	Stock de combustibles e insumos planta eléctrica, UPS.	
	Mantenimiento a los sistema de alimentación de energía planta eléctrica, UPS.	
	Sistema de iluminación de emergencia	
	Enlaces de comunicación redundantes voz, datos e internet	
Mantenimiento de hardware	Mantenimiento de equipos de acuerdo a las recomendaciones del proveedor	Errores de mantenimiento/actualización hardware (equipos)
	Personal calificado y autorizado realiza el mantenimiento de equipos	
	Registro de eventos y mantenimientos de los equipos	

Delimitación física centro de datos	Control de acceso al centro de datos y sitios donde se encuentren equipos informáticos	Acceso no autorizado
	Acceso a centro de datos solo a personal autorizado	
Control de acceso físico	Horarios de acceso al centro de datos	
	Registro de control de acceso al centro de datos	
	Autorizar el acceso de personas externas	
	Registro de control de accesos de personas externas al centro de datos	
Ubicación y protección de equipos (servidores, escritorio)	Ubicación adecuada del centro de datos en el edificio , evitando desastres naturales o contingencias	Desastres naturales
	Sistema de monitoreo de temperatura y humedad en el centro de datos	Fuego
	Sistema de detección y control (extintores) de incendios centro de datos	
	Agentes de seguridad ocupacional responsables de evacuación y manejo de desastres	
	Mantenimiento periódico de instalaciones eléctricas	
	Sistema de desagües y alcantarillados revisados periódicamente	Inundaciones
	Mantenimiento de tubería agua	
	Los equipos de escritorio poseen tomas eléctricas adecuadas, evitando cableado improvisado	Cortes de suministro de energía
	Mantenimiento periódico de las tomas eléctricas para los equipos	
	Sistema de alimentación de energía con protección UPS centralizado, provee energía 10m aproximadamente.	
	Equipos servidores alimentados por UPS exclusivo que provee energía por 30m aproximadamente	
	Luces de emergencia ubicadas dentro del centro de datos	
	Tomas eléctricas con conexión a tierra	Sobrecarga y fluctuaciones eléctricas
	Tomas eléctricas reguladas proveen voltajes de 110 y 220 voltios	
Cableado Estructurado	Cableado de datos separado del cableado eléctrico	Ataque destructivo
	Etiquetado de cables datos y eléctrico	

	Uso de gabinetes con seguridades en las áreas de intercambio o bifurcación del cableado	
	Protección del cableado tubería, canaleta, etc.	
	Control de acceso a los gabinetes de distribución para nuevas conexiones, reparaciones.	
Documentación de procesos de operación	Procedimientos documentados servicios críticos:	Errores de configuración / errores de administrador / errores de mantenimiento, actualización hardware, software
	Base de datos	
	Aplicaciones	
	Correo	
	Servicios web	
	Política de respaldos de la información	
	Relación entre aplicaciones y equipos	
	Estimación de tiempos de configuración de equipos y levantar servicios	
	Registro de problemas y soluciones a implementar	
	Contactos de proveedores y niveles de escalamiento	
	Procedimientos para reinicio de servicios y equipos, dependencias.	
Segregación de funciones	Definición de responsables y backups de los servicios y equipos críticos de la institución	

SALVAGUARDAS IDENTIFICADAS PARA EL TIPO DE ACTIVO SOFTWARE

Tabla 25
Salvaguardas activo software

Control	**Descripción del control / salvaguarda**	**Amenazas mitigadas**
Inventario de activos	Registro de aplicaciones instaladas	Errores de mantenimiento/actualización de software
	Descripción de aplicaciones	
	Equipos donde se encuentran ejecutándose	
	Respaldos y repositorios locales	
	Uso de aplicaciones	
	Responsables técnicos y operativos	
Gestión de cambios(actualización software)	Procedimientos y controles de seguridad para selección y adquisición de software	
	Socialización actualización de aplicaciones	
	Análisis de requerimientos de hardware necesarios actualización	
	Pruebas y afinamiento de las aplicaciones	

Gestión de cambios(nuevo software)	Análisis de requerimientos y justificación	
	Autorización	
	Análisis de requerimientos de hardware necesarios actualización	
	Documentación de uso y técnica	
	Instaladores, código fuente, licencias	
	Soporte técnico, actualización y mantenimiento	
	Ventanas de mantenimiento, reducir impacto	
	Capacitación	
Software de gestión infraestructura	Actualización de firmware por parte del personal calificado.	
	Documentación de configuración y manejo	
	Responsables de la administración y monitoreo	
	Requerimientos funcionalidad	
Código fuente	Repositorio centralizado	
	Control de acceso y asignación de credenciales	
	Responsables del código fuente	
	Registro de versiones y control de cambios	
Validación software	Validación de funcionamiento por parte de los involucrados	Vulnerabilidad en los programas de software
	Validación de seguridades	
	Validación de rendimiento y concurrencia	
	Verificación de fuentes, base de datos y especificaciones técnicas solicitadas	
Validación input data	Procedimiento de uso del equipo de escritorio	Errores de usuario / acceso no autorizado
	Validación de campos obligatorios	
	Control de información a ingresar	
Control de acceso	Asignación de perfiles y roles de acceso y manejo	
	Actualización y validación de credenciales	
Validación output data	Mecanismos de verificación de resultados de información sean correctos	Ingreso información incorrecta
	Reportes actualizados y coherentes	
Control procesamiento interno aplicaciones	Logs de auditoria de transacciones en las aplicaciones	Errores del usuario
	Catálogo de eventos o errores del sistema	
	Validación de la salud de las bases de datos con el fin de evitar corrupción en la información	
Ambientes de pruebas y producción	Mantener ambiente de pruebas y producción separados	Manipulación de aplicaciones, alteración de

	Verificación y control de dependencias entre aplicaciones y equipos	información, ingreso de información, control de acceso, validación de perfiles.
	Responsables de cada uno de los ambientes	
Gestión de recursos	Aplicaciones de monitoreo de los recursos de los equipos servidores que alojan las aplicaciones y servicios	Caída de sistema falta de recursos, fallos o averías físicas o lógicas, indisponibilidad del personal
	Definición de umbrales mínimo y máximo de control de recursos	
	Registro de eventos para dimensionar nuevos recursos de ser necesarios	
Controles contra código malicioso	Política sobre el uso e instalación de software no autorizado	Difusión de software dañino
	Instalación de antivirus, administración y actualización centralizada	
	Responsables del monitoreo y control de software dañino	
Seguridad documentación software	Almacenamiento de la documentación de las aplicaciones bajo llave con acceso restringido	Vulnerabilidad de los programas, manipulación de la configuración.
	Registro de la documentación almacenada	
Transacciones en línea	Manejo de protocolos de comunicación seguros, ssl	Alteración de la información, degradación de la información
	Validación de credenciales	
	Repositorio de información y credenciales de acceso ubicados dentro la intranet	
	Implementación de firmas digitales	
	Auditoria y registro de todas las transacciones realizadas	
Publicar información permitida	Servicios web donde se publica información de carácter público	Acceso no autorizado, suplantación de identidad, alterar información, degradación de la información
	Seguridad en los equipos para evitar accesos no autorizados a nivel local y de la intranet	
Registro de auditorias	Registro de accesos, control de cambios, transacciones y eventos	Acceso no autorizado.
	Registro de intentos fallidos de acceso	
	Registro de violación de accesos establecidos	
	Registro de eventos y alarmas en el centro de datos	

Política de control de acceso	Procedimiento para la gestión y autorización de acceso al centro de datos	
	Se prohíbe el ingreso de todas las personas excepto las autorizadas	
	En caso de incidentes se revocan los accesos a los responsables	
Registro de usuarios	Asignación de usuario y clave de acceso personales a los usuarios	
	Proceso de generación de usuarios y claves	
	Mantenimiento y depuración de cuentas de usuarios	
	Políticas del correcto uso y sanciones en caso de mal uso de credenciales	
Gestión de credenciales	Cambio obligatorio de clave en primer acceso del usuario	
	Procedimiento de verificación de identidad en caso de solicitar reseteo de claves	
	Almacenamiento de credenciales en el servidor formato cifrado	
	Las credenciales por defecto son actualizadas y documentadas en caso de accesos administradores	
Usuario desatendido	Política de bloqueo de equipo por parte del usuario y directiva del controlador de dominio de bloquear automáticamente en cierto periodo de inactividad	
	Las aplicaciones poseen un timeout de inactividad de 10 minutos para bloquearse	
Servicios de red	Política donde se define el uso y restricciones de la conexión con la red de datos de la institución	
	Se posee control de conectividad de los usuarios a la red mediante vlans	
	Los usuarios solo pueden acceder a los equipos y o aplicaciones autorizadas	
	Diagrama de red actualizado	
	Se posee herramienta para el monitoreo de red	
Control de accesos remotos	Políticas y procedimientos establecidos para el acceso remoto	
	Control de acceso remoto definido por el responsable quien habilita permisos de acceso temporalmente	

Segregar redes	Se deben configurar vlans que permitan separar y controlar el acceso únicamente a los recursos necesarios desde la intranet como desde el exterior.	
	Limitar el acceso a recursos autorizados y no autorizados por parte de externos	
	Mantener un sistema de monitoreo que permita conocer los accesos e intentos de acceso fallidos a la red.	

SALVAGUARDAS IDENTIFICADAS PARA EL TIPO DE ACTIVO DATOS

Tabla 26
Salvaguardas activo datos

Control	**Descripción del control / salvaguarda**	**Amenazas mitigadas**
Respaldo de información	Política del plan de respaldos de la información (periodo, tipo, tiempo almacenamiento)	Errores de usuarios, alterar información, ingreso información incorrecta, destrucción y degradación de la información
	Registro de ejecución de las tareas de respaldo, fecha, hora, responsable, tamaño, etc.	
	Lugar físico seguro donde se almacenan los respaldos de información.	
	Pruebas de restauración de respaldos medir tiempo e integridad de la información	
Computadoras	Los funcionarios deben respaldar la información importante con la que trabajen.	Daños físicos
	Los respaldos deben ser guardados en un repositorio o fileserver y en medios portátiles.	
Documentación TI	La documentación es archivada bajo llave y adicionalmente es digitalizada y almacenada en el repositorio	Destrucción de información, robo

2.4 Estimación del Estado de Riesgo

2.4.1 Estimación del Impacto.

Se denomina impacto al efecto que provoca una amenaza sobre un activo. EL impacto es una situación a la que queda expuesto el sistema

(servicios, aplicaciones, etc.) después de ser gestionado mediante el despliegue de las respectivas salvaguardas o sin la aplicación de las mismas. A continuación se procede a indicar los tipos de impacto a los que son expuestos los activos:

- Impacto Potencial.- es el impacto al que está expuesto un sistema o proceso sin la aplicación de salvaguardas a los activos.
- Impacto Residual.- es el impacto al que está expuesto un sistema o proceso aplicando las salvaguardas a los activos.

A continuación se presenta la escala que será útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

- MB: muy bajo
- B: bajo
- M: medio
- A: alto
- MA: muy alto

Tabla 27
Estimación del impacto

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Recuperado de (Amutio Gómez, Candau, & Mañas, MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas, 2012)

2.4.2 Estimación del Riesgo en Aplicaciones e Infraestructura

Se debe estimar la frecuencia con que se presentarán los riesgos identificados, así como también se debe cuantificar la probable pérdida de servicios que ellos pueden ocasionar; una vez identificados los riesgos de la institución debe procederse a su análisis, para lo cual se debe realizar lo siguiente:

- Estimación de su frecuencia.
- Valoración de la pérdida.

Finalmente se concluye que aquellos riesgos que se presenten esporádicamente no representan mayor preocupación para la institución; pero los riesgos que se presenten frecuentemente deben ser tratados de manera urgente y darles toda la atención del caso.

Tabla 28
Escala de valoración riesgo

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Recuperado de (Amutio Gómez, Candau, & Mañas, MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas, 2012).

Tabla 29
Combinación impacto y frecuencia para calculo riesgo

riesgo		*probabilidad*				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Recuperado de (Amutio Gómez, Candau, & Mañas, MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas, 2012).

Riesgo Potencial y riesgo Residual: TIPO DE ACTIVOS INFRAESTRUCTURA

Tabla 30
Riesgos activos infraestructura

ACTIVO	AMENAZA	IMPACTO	RIESGO POTENCIAL	RIESGO RESIDUAL
Equipos Portátiles	Fuego	muy bajo	despreciable	despreciable
	Desastres naturales	muy bajo	despreciable	despreciable
	Corte suministro eléctrico	muy bajo	despreciable	despreciable
	Sobrecarga y fluctuaciones eléctricas	muy bajo	despreciable	despreciable
	Avería origen físico o lógico	bajo	despreciable	despreciable
	Errores de configuración, administrador	muy bajo	despreciable	despreciable
	Robo	bajo	bajo	despreciable
	Acceso no autorizado, manipulación información	muy bajo	despreciable	despreciable
	Agotamiento de recursos	bajo	bajo	despreciable

	Errores de mantenimiento y actualización	muy bajo	despreciable	despreciable
	Ataque destructivo	muy bajo	despreciable	despreciable
	Uso no previsto	muy bajo	despreciable	despreciable
	Condiciones inadecuadas temperatura, humedad	muy bajo	despreciable	despreciable
Equipos de Escritorio	Fuego	muy bajo	despreciable	despreciable
	Desastres naturales	muy bajo	despreciable	despreciable
	Corte suministro eléctrico	muy bajo	despreciable	despreciable
	Sobrecarga y fluctuaciones eléctricas	muy bajo	despreciable	despreciable
	Avería origen físico o lógico	bajo	bajo	despreciable
	Errores de configuración, administrador	bajo	bajo	despreciable
	Robo	bajo	bajo	despreciable
	Acceso no autorizado, manipulación información	muy bajo	despreciable	despreciable
	Agotamiento de recursos	bajo	bajo	despreciable
	Errores de mantenimiento y actualización	muy bajo	despreciable	despreciable
	Ataque destructivo	muy bajo	despreciable	despreciable
	Uso no previsto	muy bajo	despreciable	despreciable
	Condiciones inadecuadas temperatura, humedad	muy bajo	despreciable	despreciable
Equipos servidores	Fuego	alto	importante	importante
	Desastres naturales	alto	importante	importante

	Corte suministro eléctrico	medio	apreciable	bajo
	Sobrecarga y fluctuaciones eléctricas	bajo	bajo	despreciable
	Avería origen físico o lógico	muy alto	critico	apreciable
	Errores de configuración, administrador	muy alto	critico	importante
	Robo	alto	importante	apreciable
	Acceso no autorizado, manipulación información	alto	importante	apreciable
	Agotamiento de recursos	muy alto	critico	apreciable
	Errores de mantenimiento y actualización	muy alto	critico	importante
	Ataque destructivo	medio	apreciable	apreciable
	Uso no previsto	alto	importante	apreciable
	Condiciones inadecuadas temperatura, humedad	medio	apreciable	bajo
Equipos de comunicación	Fuego	bajo	bajo	despreciable
	Desastres naturales	bajo	bajo	despreciable
	Corte suministro eléctrico	muy bajo	despreciable	despreciable
	Sobrecarga y fluctuaciones eléctricas	muy bajo	despreciable	despreciable
	Avería origen físico o lógico	medio	apreciable	bajo
	Errores de configuración, administrador	medio	apreciable	bajo
	Robo	medio	apreciable	bajo

	Acceso no autorizado, manipulación información	bajo	bajo	despreciable
	Agotamiento de recursos	medio	apreciable	bajo
	Errores de mantenimiento y actualización	muy bajo	despreciable	despreciable
	Ataque destructivo	muy bajo	despreciable	despreciable
	Uso no previsto	muy bajo	despreciable	despreciable
	Condiciones inadecuadas temperatura, humedad	muy bajo	despreciable	despreciable
Lugar, sitio	Fuego	medio	apreciable	apreciable
	Desastres naturales	bajo	bajo	bajo
	Acceso no autorizado	medio	apreciable	bajo
	Falta de mantenimiento	bajo	bajo	despreciable
	Ataque destructivo	bajo	bajo	despreciable
	Daños por agua	bajo	bajo	despreciable
	Condiciones inadecuadas temperatura, humedad	muy bajo	despreciable	despreciable

Riesgo Potencial y riesgo Residual: TIPO DE ACTIVO SOFTWARE

Tabla 31
Riesgos activo software

ACTIVO	AMENAZA	IMPACTO	RIESGO POTENCIAL	RIESGO RESIDUAL
Paquetes de software	Errores de los usuarios	medio	apreciable	bajo
	Errores del administrador	alto	importante	apreciable
	Errores de configuración	alto	importante	apreciable

	Difusión software dañino	muy alto	apreciable	bajo
	Escapes de información	bajo	despreciable	despreciable
	Vulnerabilidad software	alto	importante	apreciable
	Errores de mantenimiento, actualización de software	alto	importante	apreciable
	Manipulación de la configuración	bajo	despreciable	despreciable
	Suplantación de la identidad de usuario	alto	importante	apreciable
	Manipulación de programas	alto	importante	apreciable
	Uso no previsto	alto	importante	apreciable
Sistema operativo	Errores de los usuarios	bajo	despreciable	despreciable
	Errores del administrador	alto	importante	apreciable
	Errores de configuración	alto	importante	apreciable
	Difusión software dañino	muy alto	apreciable	bajo
	Vulnerabilidad software	alto	importante	apreciable
	Errores de mantenimiento, actualización de software	alto	importante	apreciable
	Manipulación de la configuración	bajo	despreciable	despreciable
	Suplantación de la identidad de usuario	alto	importante	apreciable
	Manipulación de programas	alto	importante	apreciable
	Falta de capacidad de restauración	alto	importante	apreciable

	Uso no previsto	alto	importante	apreciable
Sistema Talento humano	Errores de los usuarios	medio	apreciable	bajo
	Errores del administrador	alto	importante	apreciable
	Errores de configuración	alto	importante	apreciable
	Difusión software dañino	medio	apreciable	bajo
	Escapes de información	alto	importante	apreciable
	Vulnerabilidad software	muy alto	critico	importante
	Errores de mantenimiento, actualización de software	muy alto	critico	importante
	Acceso no autorizado	muy alto	critico	importante
	Manipulación de la configuración	alto	importante	apreciable
	Suplantación de la identidad de usuario	alto	importante	apreciable
	Manipulación de programas	medio	apreciable	bajo
Sistema Financiero	Errores de los usuarios	medio	apreciable	bajo
	Errores del administrador	alto	importante	apreciable
	Errores de configuración	alto	importante	apreciable
	Difusión software dañino	medio	apreciable	bajo
	Escapes de información	alto	importante	apreciable
	Vulnerabilidad software	muy alto	critico	importante

	Errores de mantenimiento, actualización de software	muy alto	critico	importante
	Acceso no autorizado	muy alto	critico	importante
	Manipulación de la configuración	alto	importante	apreciable
	Suplantación de la identidad de usuario	alto	importante	apreciable
	Manipulación de programas	medio	apreciable	bajo
Sistema Gestión penitenciaria	Errores de los usuarios	bajo	despreciable	despreciable
	Errores del administrador	alto	importante	apreciable
	Errores de configuración	alto	importante	apreciable
	Difusión software dañino	muy alto	apreciable	bajo
	Vulnerabilidad software	alto	importante	apreciable
	Errores de mantenimiento, actualización de software	alto	importante	apreciable
	Manipulación de la configuración	bajo	despreciable	despreciable
	Suplantación de la identidad de usuario	alto	importante	apreciable
	Manipulación de programas	alto	importante	apreciable
	Falta de capacidad de restauración	alto	importante	apreciable
	Uso no previsto	alto	importante	apreciable
Sistema gestión documental	Errores de los usuarios	bajo	despreciable	despreciable
	Errores del administrador	alto	importante	apreciable

	Errores de configuración	alto	importante	apreciable
	Difusión software dañino	muy alto	apreciable	bajo
	Vulnerabilidad software	alto	importante	apreciable
	Errores de mantenimiento, actualización de software	alto	importante	apreciable
	Manipulación de la configuración	bajo	despreciable	despreciable
	Suplantación de la identidad de usuario	alto	importante	apreciable
	Manipulación de programas	alto	importante	apreciable
	Falta de capacidad de restauración	alto	importante	apreciable
	Uso no previsto	alto	importante	apreciable
Sistema gestión de bienes	Errores de los usuarios	bajo	despreciable	despreciable
	Errores del administrador	alto	importante	apreciable
	Errores de configuración	alto	importante	apreciable
	Difusión software dañino	muy alto	apreciable	bajo
	Vulnerabilidad software	alto	importante	apreciable
	Errores de mantenimiento, actualización de software	alto	importante	apreciable
	Manipulación de la configuración	bajo	despreciable	despreciable
	Suplantación de la identidad de usuario	alto	importante	apreciable
	Manipulación de programas	alto	importante	apreciable

	Falta de capacidad de restauración	alto	importante	apreciable
	Uso no previsto	alto	importante	apreciable

Riesgo Potencial y riesgo Residual: TIPO DE ACTIVOS SERVICIOS

Tabla 32
Riesgos activos servicios

ACTIVO	AMENAZA	IMPACTO	RIESGO POTENCIAL	RIESGO RESIDUAL
Internet	Denegación de servicio	alto	importante	apreciable
	Manipulación de configuración	medio	apreciable	bajo
	Uso no previsto	medio	apreciable	bajo
	Agotamiento de recursos	alto	importante	apreciable
	Errores de los usuarios	bajo	despreciable	despreciable
	Errores del administrador	muy alto	critico	importante
	Indisponibilidad del personal	muy alto	critico	importante
	Errores de configuración	muy alto	critico	importante
Intranet	Repudio	medio	apreciable	bajo
	Denegación de servicio	alto	importante	apreciable
	Manipulación de configuración	medio	apreciable	bajo
	Uso no previsto	medio	apreciable	bajo
	Agotamiento de recursos	alto	importante	apreciable
	Acceso no autorizado	alto	importante	apreciable
	Errores del administrador	muy alto	critico	importante
	Indisponibilidad del personal	muy alto	critico	importante
	Errores de configuración	muy alto	critico	importante

Comunicaciones	Repudio	bajo	bajo	bajo
	Denegación de servicio	muy alto	critico	importante
	Manipulación de configuración	muy alto	critico	importante
	Uso no previsto	alto	importante	apreciable
	Agotamiento de recursos	muy alto	critico	importante
	Errores del administrador	muy alto	critico	importante
	Indisponibilidad del personal	muy alto	critico	importante
	Errores de configuración	muy alto	critico	importante
Portal web	Repudio	medio	apreciable	bajo
	Denegación de servicio	alto	importante	apreciable
	Manipulación de configuración	alto	importante	apreciable
	Uso no previsto	alto	importante	apreciable
	Agotamiento de recursos	muy alto	critico	importante
	Acceso no autorizado	muy alto	critico	importante
	Errores del administrador	alto	importante	apreciable
	Indisponibilidad del personal	muy alto	critico	importante
	Errores de configuración	muy alto	critico	importante
Correo electrónico	Repudio	medio	apreciable	bajo
	Denegación de servicio	alto	importante	apreciable
	Manipulación de configuración	alto	importante	apreciable
	Agotamiento de recursos	bajo	despreciable	despreciable
	Errores usuario	bajo	despreciable	despreciable
	Acceso no autorizado	muy alto	critico	importante

	Errores del administrador	alto	importante	apreciable
	Indisponibilidad del personal	bajo	despreciable	despreciable
	Errores de configuración	muy alto	critico	importante
Soporte técnico	Repudio	muy bajo	despreciable	despreciable
	Denegación de servicio	alto	importante	apreciable
	Manipulación de configuración	muy alto	critico	importante
	Uso no previsto	medio	apreciable	bajo
	Agotamiento de recursos	medio	apreciable	bajo
	Errores del usuario	bajo	despreciable	despreciable
	Errores del administrador	muy alto	critico	importante
	Indisponibilidad del personal	muy alto	critico	importante
	Errores de configuración	muy alto	critico	importante

Riesgo Potencial y riesgo Residual: TIPO DE ACTIVO DATOS

Tabla 33
Riesgos activos datos

ACTIVO	AMENAZA	IMPACTO	RIESGO POTENCIAL	RIESGO RESIDUAL
Soporte electrónico	Fuego	alto	importante	apreciable
	Desastres naturales	alto	importante	apreciable
	Corte suministro eléctrico	medio	apreciable	bajo
	Sobrecarga y fluctuaciones eléctricas	medio	apreciable	bajo
	Avería de origen físico o lógico	medio	apreciable	Bajo
	Robo	alto	importante	Apreciable
	Acceso no autorizado	bajo	despreciable	despreciable

	Ataque destructivo	medio	apreciable	bajo
	Uso no previsto	medio	apreciable	bajo
	Condiciones inadecuadas de temperatura y humedad	medio	apreciable	bajo
Documentación y registros	Fuego	alto	importante	apreciable
	Desastres naturales	alto	importante	apreciable
	Avería de origen físico o lógico	alto	importante	apreciable
	Robo	alto	importante	apreciable
	Acceso no autorizado	alto	importante	apreciable
	Ataque destructivo	alto	importante	apreciable
	Uso no previsto	alto	importante	apreciable
	Condiciones inadecuadas de temperatura y humedad	alto	importante	apreciable
Bases de datos	Errores de los usuarios	muy alto	critico	importante
	Alteración de la información	alto	importante	apreciable
	Ingreso información incorrecta	muy alto	critico	importante
	Degradación de información	muy alto	critico	importante
	Destrucción de información	muy alto	critico	importante

3 Análisis e Impacto

3.1 Análisis de la Situación actual de la red

Se procede a realizar el levantamiento del estado actual de la infraestructura de red de la institución; el levantamiento de la información será realizado en base a la documentación existente, así como a la inspección física de la misma.

3.1.1 Ubicación Geográfica de la Institución y sus dependencias.

El Ministerio de Justicia, Derechos Humanos y Cultos cuenta con un sitio matriz ubicado en Quito y varias dependencias ubicadas a nivel nacional, a continuación se proceden a enunciarlas:

- Casa de confianza Quito
- CDP Quito
- Contraventores Quito
- Flagrancia Quito
- Centro de rehabilitación Social Esmeraldas Varones
- Centro de rehabilitación Social Esmeraldas Femenino
- Centro de rehabilitación Social Tulcán
- Centro de rehabilitación Social Ibarra
- Centro de rehabilitación Social Sucumbíos
- Centro de rehabilitación Social Archidona

- Centro de rehabilitación Social El rodeo Manabí
- Centro de rehabilitación Social Femenino Portoviejo
- Centro de rehabilitación Social Quevedo
- Centro de rehabilitación Social Santo Domingo
- Centro de rehabilitación Social Babahoyo
- Centro Regional Latacunga
- Centro de rehabilitación Social Ambato
- Centro de rehabilitación Social Riobamba
- Centro de rehabilitación Social Macas
- Centro de rehabilitación Social Guaranda
- Centro de rehabilitación Social Cañar
- Centro de rehabilitación Social Azogues
- Centro Regional Cuenca
- Centro Regional Guayas
- CDP Guayaquil
- Centro de rehabilitación Social Guayas Femenino
- Flagrancia Guayaquil
- Centro de rehabilitación Social Machala
- Centro de rehabilitación Social Loja
- Centro de rehabilitación Social Zamora

Para efectos de este caso de estudio y en virtud de que el centro de datos se encuentra ubicado en el edifico matriz de la institución se procederá a realizar el análisis de la red del edificio de planta central matriz. El edificio

matriz se encuentra ubicado en la avenida Colón y Reina Victoria Esquina, la institución ocupa los siguientes pisos o plantas:

- Planta Baja
- Mezzanine

El centro de datos se encuentra ubicado en el Mezzanine donde únicamente se tiene acceso mediante un usuario y clave que es validado por el sistema de control de accesos.

3.1.2 Infraestructura de Red de la Institución.

Se realiza un análisis de las tareas y funciones que ejecutan tanto los equipos de red como los equipos servidores y enlaces de comunicaciones. Es necesario establecer y definir los responsables de cada uno de los componentes de la infraestructura tecnológica de la institución. El diagrama de red que se muestra en la figura 14 indica la disposición de cada uno de los equipos de red así como su respectiva conexión dentro de la institución.

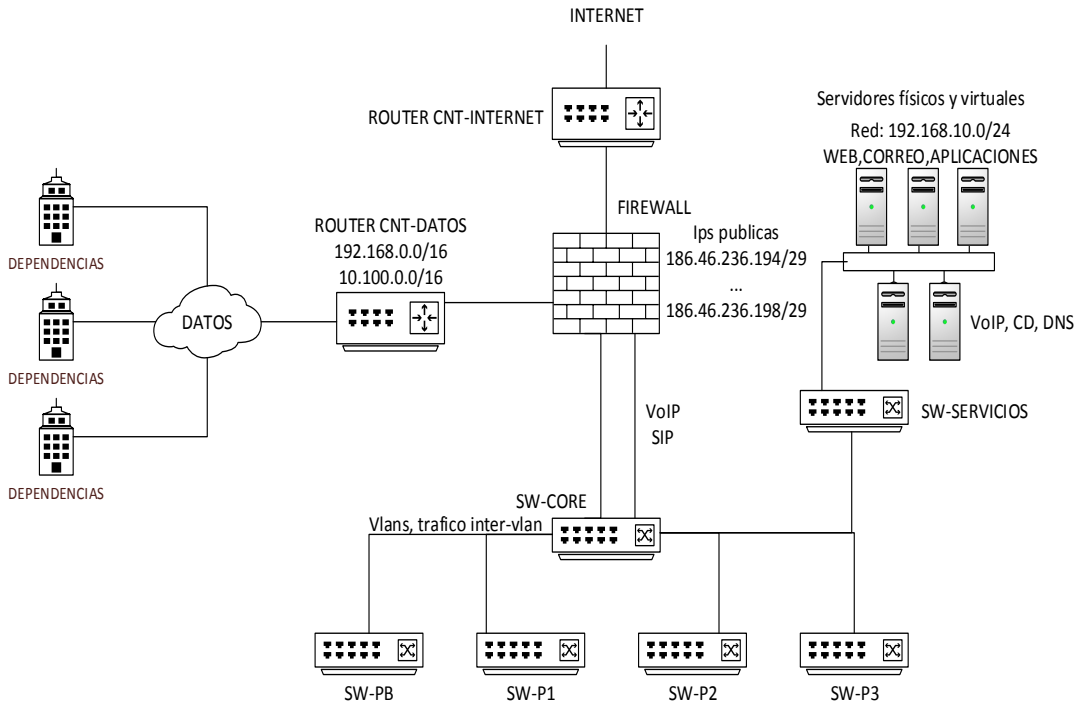


Figura 14. Diagrama de red de la institución.

3.1.2.1 Servicios.

Aplicaciones.- Las aplicaciones de la institución están montadas en un servidor HP BL460C G6 el cual posee los recursos suficientes (memoria, procesamiento y almacenamiento) para solventar la concurrencia de peticiones, la plataforma base o sistema operativo es Centos 6, las aplicaciones están desarrolladas en lenguajes java y php, las mismas que son de propiedad intelectual de la institución.

Base de Datos.- Las bases de datos son almacenadas en un servidor HP DL380 G5, el cual posee los recursos suficientes (memoria, procesamiento y almacenamiento) para solventar la concurrencia de

peticiones, la plataforma base o sistema operativo es Centos 6. Las bases de datos que son albergadas en este servidor son MySql y PostGres, que son accedidas desde el servidor de aplicaciones y controladas o mantenidas por los responsables de las aplicaciones.

Servicios Web.- El portal web de la institución está alojado en un servidor HP BL460C G6, el cual contiene la página web de la institución, así como el portal de la Intranet donde se cuelgan los servicios de la institución para los funcionarios. El portal web está desarrollado sobre Joomla y php el cual es administrado por el web master de la institución. Posee un sistema operativo Centos 6.

Correo electrónico.- El servidor de Correo Electrónico es Exchange 2012 y se encuentra sobre la plataforma Windows 2012 server. El servicio del servidor de correo (incluye POP3 e IMAP), aplicaciones, HTTP, NNTP, LDAP y Servicios Web y el repositorio de datos o mailbox se encuentra sobre sqlserver.

Directorio Activo.- Este servidor tiene instalado el sistema operativo Windows 2012 Server y habilitado el controlador de dominio, para dar acceso a los recursos del dominio y aplicación de políticas de control, acceso, seguridad, etc… a los funcionarios de la institución tanto del edificio matriz como de las dependencias a nivel nacional. Para ello se tiene el equipo HP

BL460C G6 en el cual se encuentra configurado el Controlador de Dominio y el servicio DNS.

Antivirus.- Se posee una consola de antivirus Kaspersky, la cual está instalada sobre un servidor HP BL460C G6 con Windows 2012 server, mediante el cual provee a los funcionarios de la institución realizar las actualizaciones de la base de datos de antivirus así como la difusión de las últimas actualizaciones de software.

3.1.2.2 Arquitectura de la red.

Es necesario conocer la arquitectura de red de la institución que permitirá el acceso de los funcionarios a los servicios y aplicaciones desde el edificio matriz y a nivel nacional, a continuación su arquitectura:

Capa de Acceso.- Esta capa constituye la red Lan y es la que proporciona la conexión entre el equipo del usuario y la red. Las conexiones de red de los equipos de los usuarios de cada piso del edificio matriz llegan a los armarios de comunicaciones que están dispuestos en sitios estratégicos de los pisos. Los armarios de comunicaciones albergan el rack, y este a su vez switches, patchpanel y odf de fibra que permiten la conexión al centro de datos. El cableado estructurado de la red del edificio es cable UTP categoría 6 certificados, en la actualidad con el fin de abastecer la demanda y futuro crecimiento del personal se cuenta con un 10% de puntos de datos adicionales. En la institución se encuentran 465 funcionarios con sus

respectivos computadores los cuales están ubicados en la planta baja y mezzanine respectivamente.

Capa de Core / Núcleo.- Esta capa permite el paso del tráfico de red dentro del edifico matriz desde la capa de acceso hacia la capa de servicios donde se encuentran montados los servicios de la institución. En este nivel se encuentran el switch de core con características de capa 3 o administrables, el switch de core es el encargado de manejar el tráfico intervlan y de proveer la comunicación con los armarios de comunicación, que se encuentran en los diferentes pisos que cuenta el edificio. Para las conexiones entre el switch de core ubicado en el centro de datos con los armarios de comunicación se tienen montados enlaces redundantes de fibra óptica en modo activo-pasivo. Adicionalmente se posee un equipo firewall que permite la comunicación entre la red lan, wan, dmz e internet; los enlaces de comunicación tanto para internet como para los enlaces de datos con las provincias son provistas por el ISP CNT.

Capa de Servicios.- La capa de servicios se encarga de direccionar el tráfico que generan las diferentes peticiones a las aplicaciones ya sean internas o externas hacia la plataforma de servicios los cuales están alojados en los equipos servidores. Estos servicios se conocen como servicios globales o institucionales.

Capa de Comunicación.- Esta capa constituye la red WAN de la institución, la conforman las diferentes dependencias dispuestas a nivel

nacional y las instituciones gubernamentales con las cuales se comparte información; la interconexión es realizada mediante enlaces dedicados de 1Mb por Fibra Óptica que es provista por el ISP CNT. Adicionalmente en el edificio matriz se encuentra el enlace de Internet que es el encargado de proveer de este servicio a todas las dependencias a nivel nacional de la institución.

3.2 Resultados del Análisis de Red

3.2.1 Interpretación de Resultados.

El análisis de resultados permite definir el nivel de impacto que ocasionaron los riesgos causados por amenazas y las salvaguardas aplicadas para mitigar su impacto.

3.2.1.1 Objetivos.

- Analizar los resultados obtenidos del impacto y riesgo
- Establecer prioridades entre activos

3.2.1.2 Resultados Obtenidos.

Finalmente luego de haber realizado todo el proceso de análisis de riesgo, se procederá a realizar el tratamiento de los riesgos sobre los activos

críticos para la institución y establecer el nivel de tratamiento que tendrán los riesgos.

Tabla 34
Tratamiento del Riesgo de los activos críticos de la institución

Activo	**Riesgo**	**Nivel**
Equipos escritorio	Avería de origen físico o lógico del equipo	medio
	Errores de mantenimiento y actualización de equipos	medio
Equipos servidores	Fuego	alto
	Desastres naturales	alto
	Corte suministro eléctrico	bajo
	Avería de origen físico o lógico de equipos	alto
	Errores de configuración, errores de administrador	alto
	Robo	medio
	Acceso no autorizado y manipulación de la configuración	medio
	Agotamiento de recursos informáticos	medio
	Errores de mantenimiento y actualización de equipos	alto
	Ataque destructivo	medio
	Uso no previsto	bajo
	Condiciones inadecuadas de temperatura y humedad	medio
Enlaces de comunicación	Avería de origen físico o lógico de equipos	medio
	Agotamiento de recursos informáticos	medio
Lugar/sitio	Fuego	medio
	Acceso no autorizado	medio
Paquetes software	Errores de los usuarios	medio
	Errores del administrador	alto
	Errores de configuración	alto
	Vulnerabilidad del software	medio
	Errores de mantenimiento y actualización de software	medio
	Suplantación de identidad de usuario	medio
	Manipulación de programas	medio
	Uso no previsto	medio
Sistema operativo	Errores del administrador	alto
	Errores de configuración	alto
	Errores de secuencia	alto
	Vulnerabilidad del software	medio

	Errores de mantenimiento y actualización de software	medio
	Manipulación de la configuración	medio
	Suplantación de identidad de usuario	medio
	Manipulación de programas	medio
	Falta de capacidad de restauración	medio
	Uso no previsto	medio
Sistema Talento Humano, Financiero, Gestión Penitenciaria, Gestión Documental, Gestión de Bienes	Errores de los usuarios	bajo
	Errores del administrador	medio
	Errores de configuración	medio
	Errores de secuencia	alto
	Vulnerabilidad del software	medio
	Errores de mantenimiento y actualización de software	medio
	Acceso no autorizado	medio
	Manipulación de la configuración	medio
	Suplantación de identidad de usuario	medio
	Manipulación de programas	medio
Comunicaciones	Denegación de servicio	alto
	Manipulación de la configuración	alto
	Uso no previsto	alto
	Agotamiento de recursos	alto
	Errores del administrador	alto
	Indisponibilidad del personal	alto
	Errores de configuración	alto
Correo Electrónico, Soporte Técnico	Repudio	medio
	Denegación de servicio	alto
	Manipulación de la configuración	medio
	Errores del administrador	medio
	Errores de configuración	medio
Portal Web	Repudio	medio
	Denegación de servicio	alto
	Manipulación de la configuración	medio
	Uso no previsto	alto
	Agotamiento de recursos	alto
	Errores del administrador	medio
	Acceso no autorizado	medio
	Indisponibilidad del personal	medio
	Errores de configuración	medio
Soporte Electrónico	Fuego	alto
	Desastres naturales	alto
	Avería de origen físico o lógico de equipos	medio

	Robo	alto
	Ataque destructivo	medio
	Uso no previsto	medio
	Condiciones inadecuadas de temperatura y humedad	medio
Documentación y Registros	Fuego	alto
	Desastres naturales	alto
	Avería de origen físico	alto
	Robo	alto
	Acceso no autorizado	medio
	Ataque destructivo	alto
	Uso no previsto	alto
	Condiciones inadecuadas de temperatura y humedad	alto
Base de Datos	Errores de los usuarios	medio
	Alteración de la información	medio
	Ingreso de información incorrecta	medio
	Degradación de Información	medio
	Destrucción de Información	medio

4 Diseño del Plan de Contingencias

Con el fin de dar continuidad a las operaciones de la institución en caso de ocurrir un evento o incidente es necesario establecer las medidas técnicas, humanas y organizativas a ejecutar que permitirán solventar los mismos en el menor tiempo posible y reduciendo el impacto tanto para la institución como los usuarios, a continuación se presentan las medidas:

- Medidas Técnicas.- uso de tecnología e instrumentos adecuados para mitigar de manera ágil y oportuna un incidente.
- Medidas Humanas.- actividades que realizará el personal responsable en apoyo a la medida para solventar el incidente.

- Medidas Organizativas.- consiste en establecer un orden de ejecución de tareas y actividades por parte de los responsables en caso de presentarse un incidente.

4.1 Medidas Preventivas

4.1.1 Medidas aplicadas para Catástrofes Naturales.

SEGURIDAD CONTRA DESATRES NATURALES

Riesgo: Desastres Naturales como terremotos, temblores, erupciones volcánicas, etc...

Responsables: Seguridad Ocupacional, Oficial de seguridad informática.

Medidas Organizativas

- Elaborar un plan de evacuación del personal y de los equipos tecnológicos críticos de la institución de acuerdo a una escala o estimación de importancia de las aplicaciones que se encuentren alojadas.
- Trasladar los equipos a un sitio alterno o lugar donde exista menor afectación del desastre, se debe contar con el personal idóneo para esta tarea.
- Traslado de los equipos y medios de respaldo que contengan la información crítica de la institución como son discos duros, san, cintas.

- Dependiendo de los recursos de la institución se puede hacer la contratación de un sitio en la nube que este fuera del país o local donde se monte un sitio alterno con las aplicaciones más críticas de la institución las cuales serán replicadas de acuerdo a una política de sincronización de la data.

SEGURIDAD CONTRA INUNDACIONES

Riesgo: Inundaciones

Responsables: Administrativo, Oficial de seguridad informática

Medidas Técnicas

- Instalación de sensores de nivel, donde se emitan alertas al sistema de monitoreo en caso de inundaciones.
- El diseño del centro de datos debe cumplir con las normas de construcción en este caso sobre piso falso.
- Centro de datos alterno

Medidas Organizativas

- Disponer de un cronograma para el mantenimiento de las instalaciones, revisión de goteras, filtraciones de agua, ductos y drenaje, por lo menos tres veces al año.
- Elaborar procedimiento de que como proceder en caso de que los equipos se vean afectados por el agua.

4.1.2 Medidas aplicadas para Incidentes Internos.

SEGURIDAD FISICA

Riesgo: Acceso no autorizado y manipulación de la configuración

Responsables: Administrativo, Oficial de seguridad informática

Medidas Organizativas

- Se debe implementar la política donde se establezca procedimientos para el acceso de personal de la institución y de personas externas.

SEGURIDAD EN LOS PROCESOS DE LOS USUARIOS

Riesgo: Avería de origen físico o lógico de los equipos, agotamiento de recursos informáticos, difusión de software dañino, errores en la configuración, errores del administrador, acceso no autorizado y manipulación de la configuración, errores de mantenimiento y actualización, uso no previsto.

Responsables: Infraestructura, Usuarios, Personal soporte a usuarios

Medidas Técnicas

- Los sistemas y aplicaciones de la institución deben poseer la funcionalidad de control de inactividad (caducidad de sesión); se debe implementar un controlador de dominio donde se establezcan políticas de ingreso y tiempo de inactividad en los equipos.
- Capacitación permanente a los usuarios sobre el uso y manejo de las aplicaciones, socializar las normas y recomendaciones

del uso y responsabilidad del acceso y manejo de aplicaciones de la institución.

- Asignación de claves de acceso en base a roles y perfiles de los funcionarios, previamente autorizados por el director o coordinador del área requirente.

Medidas Organizativas

- Definir política de almacenamiento y respaldos de la información de los usuarios, donde se establezca la información a respaldar, tiempo de respaldo y lugar donde será almacenado la información.
- Política donde se defina la responsabilidad sobre la confidencialidad de las claves de acceso a los sistemas y equipos a su cargo.
- Política sobre el uso e instalación de software adicional al provisto por la institución, donde se realice la justificación, aprobación y autorización para la instalación del software.
- Procedimiento para la asignación de claves de acceso y validación de roles y perfiles para el manejo de las aplicaciones

DISPONIBILIDAD SERVICIOS PROVEEDORES

Riesgos: Avería de origen físico o lógico de los equipos, agotamiento de recursos informáticos, difusión de software dañino, errores en la configuración, errores del administrador, acceso no autorizado y manipulación de la configuración, errores de mantenimiento y actualización, uso no previsto.

Responsables: Infraestructura, soporte técnico a usuarios

- Se debe poseer enlaces de comunicaciones redundantes para los servicios de internet y enlaces wan con los sitios que funcionan como alternos para la institución.
- Deben poseer niveles de escalamiento para el servicio de gestión de incidentes, así como elaboración de SLA (Acuerdos de niveles de servicio) para los servicios contratados.

4.1.3 Medidas aplicadas para Infraestructura.

SEGURIDAD CONTRA INCENDIOS

Riesgo: Fuego

Responsables: Administrativo, Oficial de seguridad informática

Medidas Técnicas

- En el centro de datos principal se colocarán sensores de humo conectados a un sistema de gestión de incendios que inmediatamente iniciara con el proceso de extinción del fuego.
- En los armarios de comunicación y centros de datos serán colocados extintores de anhídrido carbónico (tipo C), los mismos que siempre deberán estar en buen estado y por ende cumplir con la vigencia de vida útil de sus componentes.
- Mantener la ducteria y mangueras contra incendio dentro del edifico en buen estado.

- Los elementos del centro de datos como racks, cajas de distribución deberán ser de material ignifugo.
- Mantenimiento de los circuitos eléctricos, cableado y cajas de distribución en buen estado, recomendable mantenimiento cada 4 meses.
- Poseer un sitio alterno de datos donde se albergan las aplicaciones e información crítica de la institución.

Medidas Humanas

- Conocimiento sobre el modo de acción en caso de incendios.
- Designar un oficial de seguridad responsable del área de TIC.
- Capacitación al personal de la institución sobre el uso de los equipos de extinción de incendios.

Medidas Organizativas

- Definir políticas sobre el uso de artefactos eléctricos
- Procedimientos y plan de evacuación en caso de incendios
- Póliza de seguros
- Teléfonos de contactos de emergencia

SEGURIDAD CONTROL DE TEMPERATURA EQUIPOS TECNOLOGICOS

Riesgo: Condiciones inadecuadas de temperatura y humedad.

Responsables: Administrativo, Oficial de seguridad informática

- El centro de datos debe poseer un sistema de monitoreo de temperatura y humedad el cual controle el aire de precisión y

este a su vez se encargue de aumentar o disminuir la emisión de aire.

- Es necesario proveer un sistema de aire acondicionado de respaldo el cual al detectar una temperatura máxima (25 grados) comience a trabajar.
- Se puede implementar una aplicación que permita monitorear los equipos que se encuentren en el centro de datos, que mediante uso de sensores en los equipos se envíen notificaciones a la aplicación y responsables.
- Establecer un plan de mantenimiento para los equipos de aire acondicionado.

HARDWARE

Riesgo: Acceso no autorizado, robo y manipulación de la configuración

Responsables: Oficial de seguridad informática

Medidas Organizativas

- La institución debe de contratar un seguro contra robo, incendio, inundaciones, daño o desastre natural o industrial, para todo el equipamiento tecnológico catalogado como bien o activo, el valor asegurado debe ser el 100% del valor del equipo.
- Política y procedimiento de control de acceso al centro de datos y demás lugares donde se encuentren equipos tecnológicos catalogados como críticos para la institución.

- Control de acceso para el personal externo a la institución debidamente aprobado y supervisado por el responsable del centro de datos.
- Definición y asignación de permisos a los funcionarios para acceso a centro de datos y demás sitios donde se encuentren equipos tecnológicos críticos de la institución.
- Política de acceso a personal no autorizado al centro de datos definiendo responsable, horarios y autorización.
- Política donde se establezca periodos de revisión de los equipos con el fin de contrastar con el inventario realizado.
- Establecer plan de mantenimiento de equipos y revisión de garantías.

Medidas Técnicas

- Control de accesos al centro de datos, es recomendable por lo menos cumplir con dos de los siguientes modos de acceso:
    - Llave
    - Usuario y clave
    - Biometría
    - Tarjeta magnética
- Implementar sistema de monitoreo de control de accesos el cual envié notificaciones a los responsables vía correo o mensaje de texto.
- Bitácora donde se registre el ingreso y egreso del personal.

CABLEADO ESTRUCTURADO

Riesgo: Avería de orden físico, agotamiento de recursos.

Responsables: Administrativo, Administrador de red TIC

Medidas Técnicas

- Poseer enlaces de backup desde el centro de datos a los armarios de comunicación y con el proveedor de servicios wan e internet.
- Inspección física de los enlaces así como pruebas de conectividad.
- Establecer responsables del mantenimiento y monitoreo de los enlaces de comunicación y cableado estructurado.

Medidas Organizativas

- Elaborar política sobre los procedimientos a realizar en caso de existir un incidente con los enlaces.
- Establecer lugar adecuado para el almacenamiento de la información de las comunicaciones de la institución.
- Establecer responsables y niveles de escalamiento para solventar incidentes con los servicios de comunicaciones wan e internet.

ACCESO A LA RED DE DATOS

Riesgos: Avería de origen físico o lógico de los equipos, agotamiento de recursos informáticos, difusión de software dañino, errores en la

configuración, errores del administrador, acceso no autorizado y manipulación de la configuración, errores de mantenimiento y actualización, uso no previsto.

Responsables: Infraestructura, Redes y personal de soporte técnico

Medidas Técnicas

- Mantener enlaces redundantes en el backbone así como en las conexiones a los equipos críticos de la institución ubicados en el centro de datos.
- La seguridad perimetral debe poseer un esquema de servicio en alta disponibilidad, esto quiere decir que en caso de fallar el firewall principal se pueda seguir trabajando con el equipo backup.
- Los puntos de datos deben ser únicamente activados cuando se vaya a conectar un equipo a la red, esto debe ser realizado por el administrador de red, previamente autorizado por el director o coordinador del área.
- Implementar la configuración de vlans que servirán para realizar el control de acceso a los servicios, equipos y aplicaciones autorizadas.
- Implementar software de monitoreo de red y aplicaciones con el fin de verificar el acceso y control de aplicaciones.
- Poseer equipos redundantes para los servicios críticos de red, en este caso servidor de controlador de dominio, servidor dns y servidor dhcp, los cuales están ubicados en otra dependencia de la institución.

- Proceso de control de cambios, documentación y registro de las configuraciones, estructura y diagramas de la red de datos.
- Política sobre el control de acceso remoto por parte de entidades externas, verificación y autorización de acceso, así como horarios y restricciones.

Medidas Organizativas

- Definición de políticas de acceso a aplicaciones en base al orgánico funcional de la institución.
- Política y procedimiento de control de acceso para conexiones remotas.

4.1.4 Medidas aplicadas para Aplicaciones.

SOFTWARE

Riesgo: Acceso no autorizado, robo y manipulación de la configuración

Responsables: Oficial de seguridad informática

Medidas Organizativas

- Se debe implementar las políticas para el acceso de los funcionarios y de ciudadanos a las aplicaciones.
- Política sobre el control de acceso y mantenimiento de los repositorios donde se encuentre alojado el código fuente y aplicaciones de la institución.

- Definir responsables de los repositorios de las aplicaciones, quien estará a cargo de la custodia y validar proceso de ingreso o egreso de la información (código fuente, aplicaciones).

Medidas Técnicas

- Inventario de software que posee la institución, el mismo que por lo menos debe contar con la siguiente información:
    - Cantidad de Software
    - Descripción del software
    - Equipos donde se encuentra instalado
    - Estado del software (activo, baja, rediseño)
    - Responsable
    - Licenciamiento
- Categorización y organización del software de acuerdo a si es código fuente o aplicación.
- Registro de ingreso o egreso de software en una bitácora, la cual debe contener por lo menos la siguiente información:
    - Revisión (contenido, cantidad, destino)
    - Objeto (comprar, probar, reemplazar, devolver, dar de baja)
    - Aprobada por el coordinador de desarrollo, persona responsable que va a recibirlo o entregarlo.
    - Registro ingreso, egreso
    - Devolución autorizada por medio de un responsable del área de desarrollo.
    - El personal técnico debe ser responsable de la manipulación del software.
    - Acta entrega recepción.
    - Acuerdos de confidencialidad.

- Elaborar política y procedimiento para el almacenamiento de la documentación de los sistemas en un lugar adecuado con las seguridades del caso.
- Crear una política y procedimientos de respaldo de los códigos fuentes y ejecutables del software de la institución, donde sus responsables garanticen su disponibilidad en caso de un evento.

GESTION DE CAMBIOS SISTEMAS INFORMATICOS

Riesgo: Errores en la configuración, errores del administrador, acceso no autorizado y manipulación de la configuración, errores de mantenimiento y actualización, uso no previsto.

Responsables: área desarrollo y control de calidad servicios informáticos

Medidas Técnicas

- Para realizar cualquier cambio se debe analizar la factibilidad y el impacto de la implantación del software en la infraestructura tecnológica, dentro de las aplicaciones y costos.
- Reuniones con las partes involucradas para revisión de avances y aceptación por parte de los funcionarios.
- Documentar todos los requerimientos del proyecto, así como actas de reuniones, manuales, etc.
- Mantener registro del control de versiones realizadas en las aplicaciones de software.

- Las actualizaciones o cambios en las aplicaciones deben ser realizadas solo por los administradores de las aplicaciones con la respectiva autorización de la dirección.
- La implementación de los cambios se deben realizar solicitando la respectiva ventana de mantenimiento y no interrumpen los procesos críticos, salvo ciertas excepciones consideradas y autorizadas por la autoridad.
- Todo el software de la institución debe de disponer de un registro o memoria técnica del desarrollo donde se detalle la fecha, hora, responsable, versiones, actas y manuales de instalación y configuración.
- En la medida de lo posible implementar un software de gestión para control de versiones ya sea de distribución libre o licenciado.

DISPONIBILIDAD DE LOS SISTEMAS INFORMATICOS

Riesgo: Avería de origen físico o lógico de los equipos, agotamiento de recursos informáticos, difusión de software dañino, errores en la configuración, errores del administrador, acceso no autorizado y manipulación de la configuración, errores de mantenimiento y actualización, uso no previsto.
Responsables: Infraestructura, aplicaciones y oficial de seguridad informática

Medidas técnicas

- Las aplicaciones críticas deberán tener documentada la información necesaria y requerida como variables, rutas, procedimientos, tips de configuración y software de monitoreo y control para levantar sus servicios.
- Las aplicaciones críticas deberán disponer de mecanismos para regreso al estado anterior (roll back) así como para restaurar el sistema antes de implementar cambios.
- Se debe identificar y establecer los parámetros o indicadores necesarios para determinar el funcionamiento correcto del sistema.
- Disponer de herramientas de monitoreo de los recursos de los equipos y aplicaciones, que permitan el envío de notificaciones (email, sms, etc.) a los responsables.
- Realizar el dimensionamiento de los recursos necesarios de hardware y software para el correcto funcionamiento de las aplicaciones, y su futuro crecimiento.
- Llevar un registro de las integraciones entre aplicaciones tanto de la propia institución como con entidades externas, esto servirá para dimensionar el impacto sobre las aplicaciones críticas de la institución.
- Definir el proceso a ejecutar para levantar los servicios y aplicaciones; se definirá la secuencia de levantamiento o

encendido de los equipos, sus componentes, servicios y tiempos estimados que le toma a cada uno estar en línea.

- Mantener un registro documentado de lecciones aprendidas donde se describa el incidente y las tareas realizadas para solucionar el incidente.

Medidas Organizativas

- Establecer responsables de las operaciones, monitoreo de las aplicaciones y ejecutar tareas para solventar los incidentes.
- Disponer de procedimientos documentados de los sistemas críticos de la institución como: bases de datos, servidor de aplicaciones, servidor de correo, servidor web, copias de seguridad y respaldo de datos e información.
- Directorio con personas técnicas de contacto y niveles de escalamiento de los incidentes en caso de necesitarlos.

AMBIENTE DE PRUEBAS Y PRODUCCION DE LOS SISTEMAS INFORMATICOS

Riesgo: Errores en la configuración, errores del administrador, acceso no autorizado y manipulación de la configuración, errores de mantenimiento y actualización, uso no previsto.

Responsables: Infraestructura, aplicaciones y oficial de seguridad informática

- Disponer de áreas de control de calidad, gestión de cambios y seguridades dentro del área de desarrollo y aplicaciones que se

encarguen de realizar la validación y pruebas de confianza de la nueva aplicación.

- Procedimiento y procesos para que una aplicación pase del ambiente de desarrollo al ambiente de producción, solicitar ventanas de mantenimiento con la respectiva anticipación.
- Definición de responsables y personal de soporte técnico para las aplicaciones.
- Procesos de seguimiento, registro y evaluación de incidentes y/o errores en el funcionamiento de la aplicación.
- Elaborar política de control de cambios, almacenamiento y respaldos de los códigos fuentes de las aplicaciones; definir procesos de restauración de respaldos y tiempos de operación.

DISPONIBILIDAD DE LOS RESPALDOS DE LA INFORMACION

Riesgos: Alteración de la Información, destrucción de Información, introducción de información incorrecta, degradación de información.

Responsables: aplicaciones, Infraestructura, oficial de seguridad informática

Medidas Técnicas

- Organizar los backups en lugares adecuados con las seguridades respectivas.
- Los backups deben ser almacenados en un lugar fuera de la institución que brinde las garantías físicas y de seguridad necesarias para su manejo y tiempo de vida.

- Otra opción consiste en generar procesos de backups que envíen la información a sitios alternos de la institución en horarios donde no se afecte el rendimiento de la red, las aplicaciones y comunicaciones.
- Se puede realizar la contratación de un sitio en la nube donde se replique la información ya sea de forma total o incremental.
- Implementar una herramienta tecnológica que permita gestionar de forma centralizada la generación de respaldos, realice el envío de notificaciones y sirva como base para la restauración de los mismos.

Medidas Organizativas

- Elaborar la política de generación de respaldos de la información donde se define el periodo y horario del respaldo así como el tipo y tiempo de vida del respaldo.
- Establecer dentro de una política de respaldo de datos que los mismos se almacenen en lugares apartados, a una distancia suficiente, que garantice que si se produce un desastre en el centro de datos principal, estos no se verán afectados.
- Los medios de respaldo deberán ser probados regularmente para asegurar que son confiables y se los puede utilizar en caso de una emergencia.
- Los procesos y procedimientos de restauración de respaldos deben ser revisados cada cierto tiempo, esto con el fin de

garantizar que son efectivos, confiables y que pueden ser completados en el tiempo estimado.

- Establecer la política donde se determine el tiempo de almacenamiento de los respaldos.

4.2 Relaciones de Coordinación del Plan de Contingencia

Es necesario coordinar con las instituciones que provean de servicios y suministros al Ministerio de Justicia, Derechos Humanos y Cultos las actividades que ayuden a minimizar el impacto y tiempo de indisponibilidad de los servicios y aplicaciones en caso de ocurrir un incidente; adicionalmente se debe coordinar las tareas y procedimientos a realizar por parte de cada una de las áreas de la institución.

4.2.1 Áreas Internas.

Áreas de la institución con las que se debe establecer la relación de coordinación:

- Redes y Comunicaciones
- Infraestructura
- Servicios y aplicaciones
- Soporte Técnico
- Administrativo
- Financiero

4.2.2 Entidades Externas.

Instituciones con las que se debe establecer la relación de coordinación:

- Proveedor de servicio de internet y enlaces de comunicaciones
- Proveedores encargados de la Infraestructura tecnológica
- Personal técnico responsables de las aplicaciones y software
- Bomberos
- Empresa eléctrica
- Proveedor de telefonía convencional y celular

4.3 Coordinador del Plan de Contingencia

El Coordinador del Plan de Contingencia es responsable de la supervisión, control y coordinación de las actividades de recuperación establecidas en este plan.

4.3.1 Definición y Responsabilidades

El Coordinador del plan es el responsable y el encargado de socializar y distribuir la información necesaria a cada uno de los involucrados en la ejecución del plan; será responsable de la actualización y registro de los eventos suscitados, así como de su almacenamiento. El coordinador del plan definirá horarios para realizar pruebas y simulacros de las actividades del plan para validar el correcto funcionamiento de las mismas; es necesario la

participación de las áreas involucradas así como de sus responsables. De los resultados obtenidos se elaboraran los respectivos documentos de lecciones aprendidas donde se registraran los resultados, y si son desfavorables será necesario redefinir los procesos que ejecuten las salvaguardas de la manera adecuada.

4.4 Organigrama del Equipo del Plan de Contingencia

Para la correcta implantación y ejecución del plan de contingencia es necesario definir una cadena de mando y sus responsables, en ese sentido es conveniente diseñar el organigrama para la ejecución del plan donde se asignaran deberes y responsabilidades de cada una de las áreas.

4.4.1 Orgánico Funcional de la Institución.

A continuación se presenta el organigrama del equipo del Plan de contingencia para el Ministerio de Justicia, Derechos Humanos y Cultos; se estableció como proceso core del negocio al proceso de Gestión Penitenciaria.

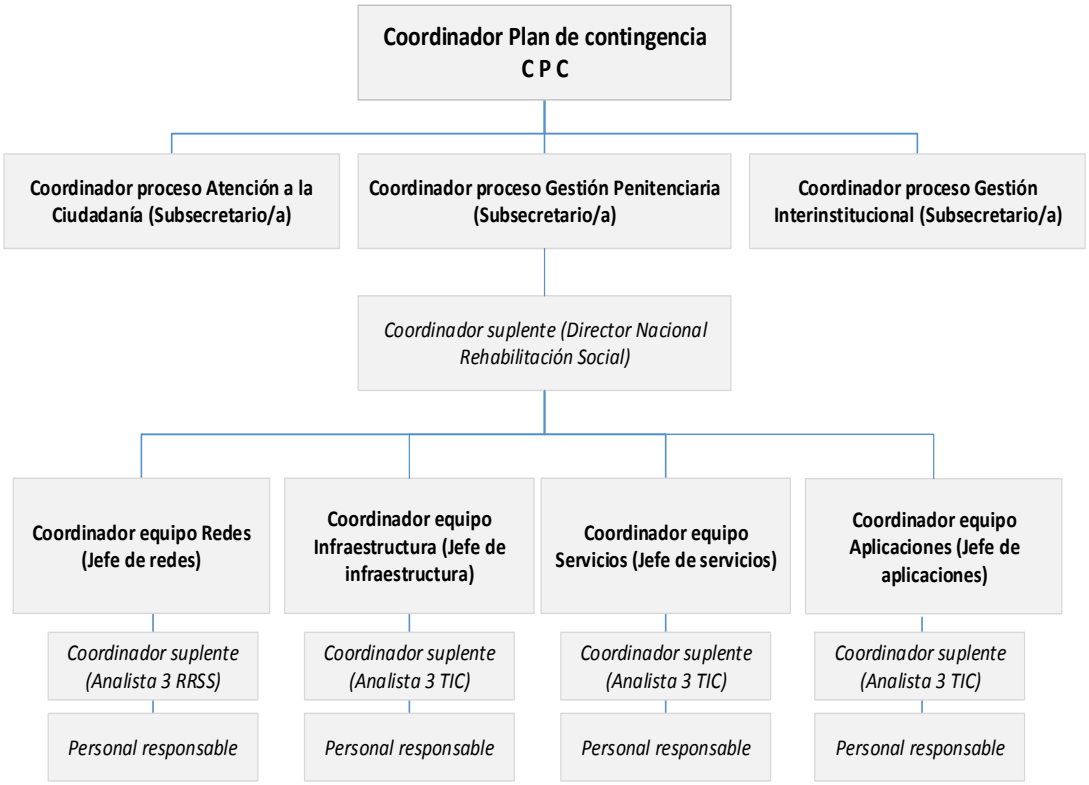


Figura 15. Organigrama Institución. Fuente: Elaborado por el autor

La designación de los coordinadores de los equipos para el plan de contingencia debe ser realizada en base a la actitud y pro actividad de los involucrados, en tal virtud el coordinador del equipo debe ser capaz de tomar decisiones, tener liderazgo y ejecutar las siguientes tareas:

- Participar en las sesiones de trabajo programadas para la evaluación de los riesgos e impactos del proceso bajo su responsabilidad.
- Liderar la recuperación del proceso a su cargo en los simulacros y prácticas, y en las situaciones reales.
- Generar y proponer recomendaciones que permitan realizar mejoras al proceso de recuperación

- Documentación y registro de los eventos y soluciones aplicadas
- Coordinar con otros equipos de recuperación.
- Tener el suficiente conocimiento sobre el proceso que lidera.
- Actuar con tranquilidad y serenidad ante un incidente

El personal responsable es el grupo técnico encargado de realizar las tareas necesarias para solventar en el menor tiempo posible un incidente, deben proceder de acuerdo a lo indicado por el coordinador del equipo.

4.4.2 Responsables de las Áreas Internas.

COORDINADOR EQUIPO DE REDES

El coordinador del equipo de redes es el encargado de ejecutar las tareas para reestablecer las comunicaciones, así como notificar al Coordinador del Plan de Contingencia sobre las interrupciones de los servicios y el estado de recuperación de los mismos. A continuación se mencionan sus principales responsabilidades:

- Diseñar la estructura de red de la institución
- Documentar los procesos de configuración de los equipos
- Mantener respaldos de las configuraciones de los equipos y realizar pruebas de restauración de los backups.
- Gestionar la disponibilidad de los servicios de internet y de los enlaces dedicados de la institución con el proveedor de servicios CNT.

- Mantener equipos, dispositivos y medios alternos de comunicación los cuales permitan reestablecer las comunicaciones en caso de daños físicos.
- Realizar pruebas y monitoreo de las comunicaciones.

COORDINADOR EQUIPO DE INFRAESTRUCTURA

El coordinador del equipo de infraestructura es el responsable de restaurar y reiniciar los equipos de infraestructura donde se alojan los servicios y aplicaciones de la institución; adicionalmente debe estar comunicando permanentemente sobre el avance y estado de los equipos al coordinador del plan de contingencia. A continuación se mencionan sus principales responsabilidades:

- Inventario de equipos.
- Registro de las configuraciones de los equipos
- Mantener respaldos de los equipos y realizar pruebas de restauración de los backups.
- Establecer proceso de restauración y dependencia de los equipos al momento de levantar la infraestructura.
- Instalar hardware provisional para solventar el incidente.
- Determinar la instalación y con figuración de hardware adicional en el sitio alterno si fuese necesario.
- Monitoreo y seguimiento del hardware del centro de datos de la institución.

- Documentación y registro de incidentes donde se indique el proceso aplicado para la resolución del mismo.

COORDINADOR EQUIPO DE SERVICIOS

El coordinador del equipo de servicios es el encargado de monitorear y organizar las tareas con las diferentes áreas de TIC para levantar los servicios y aplicaciones que ofrece la institución al ocurrir un incidente; debe estar en constante contacto con el coordinador del plan de contingencia. A continuación se mencionan sus principales responsabilidades:

- Monitorear los servicios y aplicaciones
- Registro de dependencias entre aplicaciones y equipos.
- Gestionar con los jefes de área los incidentes presentados
- Establecer procesos para definir prioridad de servicios y aplicaciones
- Documentar incidentes y operaciones realizadas.

COORDINADOR EQUIPO DE APLICACIONES

El coordinador del equipo de aplicaciones es el encargado de verificar y controlar que las aplicaciones se encuentren operativas en el menor tiempo posible; debe estar en constante contacto con el coordinador del plan de contingencia. A continuación se mencionan sus principales responsabilidades:

- Mantener un respaldo de las aplicaciones y su información.
- Inventario de aplicaciones.

- Dependencia entre aplicaciones y equipos.
- Establecer procesos de restauración de las máquinas virtuales, aplicaciones y bases de datos.
- Registro de configuraciones de los aplicaciones y equipos.
- Establecer plan de restauración de aplicaciones en infraestructura alterna y en sitio alterno.
- Coordinar con jefes de las áreas de TIC los procesos de restauración y configuración de aplicaciones.
- Registrar eventos e incidentes, así como procedimientos aplicados en la resolución de los mismos.

Finalmente se presenta el orgánico funcional del plan de contingencia con los responsables y sus competencias.

Tabla 35
Responsables de plan de contingencias TIC

Procesos y Servicios	**Sistemas / Aplicaciones**	**Equipo Redes**	**Redes**	**Equipo Infraestructura**	**Infraestructura**	**Equipo Servicios**	**Servicios**	**Equipo Aplicaciones**	**Aplicaciones**
Servicios	VPPL	Luis Montenegro / Fernando Tirado / María José Espinosa	Firewall / Switch Core, SAN / Switch Distribución, Acceso / Ancho de banda /	Maritza Onofa / Esteban Carrillo / Roberto Vaca	Servidor de aplicaciones - virtual	Gonzalo Moncayo / Mario Perea / Fernanda Rivera	Horarios de visitas	Adrián Guayasamin / Diego Pozo / Héctor Santander	Sistema de información de visitas - base datos
Nomina	R-TTHH				Servidor de aplicaciones - virtual		Información del personal		Sistema de talento humano - base datos
Bienes	Olympo				Servidor - físico		Información de		Sistema

			Wireless LAN controller / Access Point / Enlaces				activos fijos		Olympo
Compras Públicas	Sprint				Servidor de aplicaciones - virtual		Procesos compras públicas		Sistema compras publicas
Contabilidad	Sigef				Servidor de aplicaciones - virtual		Pagos		Sistema de Pagos
Jurídico	Lexis				Servidor de aplicaciones - virtual		Jurídico		Sistema de leyes jurídicas
Auditoria interna	Olympo				Servidor - físico		Información auditoria interna		Sistema de registro de procesos
Atención ciudadanía	Sirec				Servidor de aplicaciones - virtual		Registro ciudadano		Sistema de registro ciudadano
Rehabilitación Social	Sigpen				Servidor - físico Servidor - virtual		Gestión Penitenciaria		Sistema de Gestión penitenciaria - base datos
Asuntos interinstitucionales	esi-Proa				Servidor de aplicaciones - virtual		Convenios interinstitucionales		Sistema de registro de convenios y casos internacionales
Intranet	Gestión Documental - Cobus				Servidor - físico		Gestión documental		Sistema Cobus -bpm - base datos

	Video Conferencia - Pollycom				Servidor - físico		Videoconferencia		Sistema RealPrecense
	Correo electrónico - Exchange				Servidor - físico		Correo electrónico		Mail Exchange 2012 - CAS,mailbox
	Portal Web - Wordpress				Servidor de aplicaciones - virtual		Página web institución		Portal Web - base datos
	Directorio Activo / DNS				Servidor - físico		Controlador de dominio / DNS		CD Windows 2012 server

4.5 Activación del Plan de Contingencia

Es necesario elaborar un proceso de activación del plan donde se definirá el modo de comunicación y el responsable de hacerlo que se encargará de notificar a los coordinadores de equipo para proceder con la ejecución de las tareas correspondientes.

4.5.1 Aprobación.

La activación del plan de contingencia debe ser realizada por la persona designada como coordinador del plan de contingencia quien fue designado por la máxima autoridad de la institución; el Coordinador será el encargado de aprobar la activación del plan de contingencia.

4.5.2 Socialización.

El Coordinador será el encargado de notificar a los coordinadores de los equipos sobre la activación del plan de contingencia. Cada uno de los coordinadores realizará un análisis del estado actual de las operaciones y notificará al Coordinador.

4.5.3 Actividades en el inicio, durante y cierre del Plan de Contingencia.

INICIO

Luego de realizar la activación del plan de contingencia se realiza la notificación inicial a los coordinadores de equipo quienes son los encargados de participar al personal de soporte apropiado, dar asistencia en el desarrollo de las recomendaciones de recuperación y en la activación de los equipos de recuperación tanto de los procesos de negocio como de los de tecnología. Para el personal de las áreas de TIC se estableció el siguiente procedimiento:

- Notificar a los coordinadores de cada una de las áreas de TIC.
- Descripción del evento o incidente y los daños ocasionados.
- Información de contacto.
- Notificar y coordinar con el Coordinador del plan de contingencia para la ejecución de medidas.

Se debe realizar la verificación del desastre luego del incidente, la verificación es realizada de la siguiente manera:

- En la medida de lo posible realizar la verificación física del lugar para evaluar los daños ocasionados (check list del inventario de equipos y componentes del centro de datos). Se realiza la verificación del estado físico de los equipos tecnológicos, estado de respaldos físicos de la información, documentación, manuales, etc.
- Realizar la estimación de tiempo para la restauración y reanudación de los servicios en base a la inspección realizada.
- Finalmente luego de la inspección, los coordinadores de área deben reportarse con el coordinador del plan de contingencia para participar en una reunión de evaluación donde se indicaran los tiempos estimados para restaurar los servicios y coordinar la secuencia y la forma (gradual o total) de reactivación.
- El sitio de reunión debe estar ubicado en una zona segura ya sea dentro o fuera de la institución dependiendo del daño, se debe contar con los medios de comunicación necesarios para poder gestionar la ejecución del plan de contingencia.

Se debe considerar el hecho de comunicar el desastre a todas las áreas de la institución, así como a entidades externas si la situación así lo amerita.

DURANTE

El responsable del almacenamiento y gestión de backups deberá determinar junto con los jefes de infraestructura, aplicaciones y servicios el

sitio más adecuado para establecer el lugar alterno donde serán restaurados los datos; dependiendo de los daños puede ser en el mismo edificio, alguna dependencia local o remota. Es necesario realizar una evaluación profunda de los daños por parte del coordinador del plan de contingencia acompañado del coordinador de TIC y coordinador de seguridad, los cuales revisaran el estado del sitio como de la infraestructura tecnológica. La inspección debe contemplar los siguientes aspectos:

- Dependiendo del daño se deberá solicitar la autorización de la entidad de seguridad (policía, bomberos, etc.) encargada para el ingreso a las áreas e instalaciones del lugar.
- Determinar los implementos de seguridad (linternas, casco, gafas, mascarilla, guantes, etc.) necesarios para el acceso del personal al sitio, en caso de poseerlos se los deberá adquirir.
- La institución debe contar con personal de seguridad ocupacional la cual tenga conocimiento del cómo proceder en la inspección al sitio, en caso de no contar con el personal calificado se deberá solicitar el acompañamiento de la policía, cruz roja o bomberos.
- Definir tareas específicas a cumplir por el personal que va a realizar la inspección, se deberán registrar las tareas realizadas. Es fundamental que el personal designado de TIC revise la condición de los equipos de comunicación, almacenamiento, infraestructura tecnológica y comunicaciones.

Luego de realizar la inspección y determinar el estado real del sitio como de su infraestructura tecnológica se procederá a elaborar el plan y proceso de restauración de servicios que se determinó anteriormente, se emitirán las recomendaciones de las actividades a realizar tomando en cuenta la prioridad de los servicios que ayudaran a solventar el desastre de la mejor manera. Finalmente se deberá estimar el tiempo de la duración de la interrupción de los servicios y aplicaciones de TIC.

CIERRE

En la fase de cierre se deberá realizar el seguimiento del estado del evento y el reporte de las acciones de recuperación deben ser registrados por el Coordinador. A continuación se menciona algunos criterios para el registro de los mismos:

Controlar el estado del evento realizando el seguimiento a las actividades de respuesta y recuperación del personal involucrado en las mismas. Se debe considerar lo siguiente: tipo de evento, áreas afectadas, actividades ejecutadas. Documentar la bitácora del avance de las tareas en secuencia cronológica; el propósito de este reporte de estado es contribuir en el control y las comunicaciones entre las áreas de la institución.

Es fundamental que cada uno de los coordinadores de las áreas de TIC organice al personal técnico de TIC a su cargo para efectuar las tareas de soporte, configuración, restauración y monitoreo de la infraestructura

tecnológica. El coordinador de TIC debe supervisar la seguridad física del lugar, adquisición de suministros tecnológicos, contactar a los proveedores de servicios y equipos.

4.6 Infraestructura y Aplicaciones Críticas de TIC en la institución para la continuidad del negocio.

A continuación se procede a indicar los equipos tecnológicos críticos de la institución:

Tabla 36
Equipos críticos MJDHC

Orden recuperación	Recurso	Equipo recuperación
1	Firewall	Comunicaciones
1.1	Switch core	Comunicaciones
2	SAN	Operaciones
2.1	Servidor directorio activo, dns	Operaciones
2.2	servidor dhcp	Operaciones
2.3	servidor aplicaciones	Operaciones
2.4	servidor correo	Operaciones
2.5	Servidor Web	Operaciones

A continuación se procede a indicar las aplicaciones tecnológicas críticas de la institución:

Tabla 37
Aplicaciones críticas MJDHC

Área/ Unidad	Funciones afectadas	Sistema informático	Factor riesgo	TMI	TR	RPO	Criticidad
Rehabilitación Social	Personas privadas libertad	esigpen	O,C	24h	h	h	5
	Adolecentes conflicto ley	asi	O,C	24h	5h	8h	4
	Planeación	poa	I,C	48h	2h	12h	4
	Video conferencia	real precense	C	24h	8h	8h	3
	Garantías	grti	O	72h	6h	12h	3

Coordinación administrativa-financiera	Finanzas	esigef	I,C	24h	8h	8h	4
	Compras públicas	esercop	C,O	24h	8h	8h	3
	Bienes	olympo	O	48h	6h	12h	3
	Contabilidad	cntb	I,C,O	24h	6h	8h	4
Talento Humano	Nomina	itthh	O	24h	4h	8h	4
	Control de asistencia	tasiste	O	72h	2h	12h	3
Atención Ciudadanía	Consultas ciudadanía	sirec	O	24h	6h	12h	3
Todas la institución	Mensajería	open fire	C	48h	6h	8h	3
	Correo electrónico	Exchange	O,C,I	24h	8h	8h	4
	Gestión documental	Cobus	O,C,I	48h	8h	8h	3
	Portal web	Wordpress	O	24h	4h	8h	3
	Mesa de ayuda	Otrs	O	48h	6h	8h	3

Factores de riesgo sistemas informáticos:

- I: integridad
- O: operatividad
- C: confidencialidad
- TMI: tiempo máximo de interrupción
- TR: tiempo de recuperación
- RPO: tiempo de perdida de datos
- Criticidad: 5-máxima, 1-minima

4.7 Medidas de Mitigación y/o Recuperación del Desastre

4.7.1 Plan de Contingencia para los Activos de Infraestructura y Aplicaciones de la institución.

A continuación se proceden a indicar las acciones asociadas al plan de contingencia en caso de ocurrir alguno de los siguientes incidentes tanto para infraestructura como aplicaciones de la institución:

CONTINGENCIA	Fuego/Incendio
FUENTES DE RIESGO	**ESTIMACION DE RIESGO**

Infraestructura tecnológica Aplicaciones Instalaciones Equipos varios	Alto
RESPONSABLES	Oficial de seguridad informática, administrativo, coordinador TIC
ACCIONES ASOCIADAS	
1. Activación del sistema de alarmas y control de incendios. 2. Realizar evacuación del sitio. 3. Llamada de emergencia a los bomberos, cruz roja, policía, etc. 4. Desactivar suministro eléctrico. 5. Revisión de las instalaciones e infraestructura tecnológica. 6. Coordinador con el CPC la activación del plan, ejecución de procesos y actividades asignadas.	
CONTINGENCIA	Inundación
FUENTES DE RIESGO	**ESTIMACION DE RIESGO**
Infraestructura tecnológica Aplicaciones Instalaciones Equipos varios	Alto
RESPONSABLES	Oficial de seguridad informática, administrativo, coordinador TI
ACCIONES ASOCIADAS	
1.- Activación del sistema de alarmas y monitoreo. 2.- Apagar los equipos tecnológicos. 3.- Colocar los equipos, respaldos y documentación en un lugar fuera del alcance del agua, si es posible cubrirlos con plástico. 4.- Llamar a las entidades de socorro como cruz roja, bomberos, etc. 5.- Revisión de las instalaciones e infraestructura tecnológica. 6.- Coordinador con el CPC la activación del plan y ejecución de procesos y actividades asignadas. 7.- Determinar si existen daños en los equipos y servicios, los cuales pueden ser: • Hardware.- realizar pruebas de funcionamiento en caso de falla se deberá gestionar con el fabricante o vendedor el cambio del equipo o sus componentes. • Software.- revisión de sistema operativo, bases de datos y aplicaciones, en caso de ser necesario se deberá restaurar backups y analizar dependencias de otros equipos o aplicaciones. • Redes.- revisar los enlaces de comunicaciones internos y externos, en caso de fallo gestionar con el proveedor la activación de los servicios. 8.- Si la solución del incidente ya sea de hardware, software o de redes requiere de un tiempo superior a 1 día se restituirá el servicio mediante un equipo provisional.	
CONTINGENCIA	Servicios institucionales caídos
FUENTES DE RIESGO	**ESTIMACION DE RIESGO**
Infraestructura tecnológica Aplicaciones Instalaciones Equipos varios	Alto

RESPONSABLES	Oficial de seguridad informática, administrativo, coordinador TI
ACCIONES ASOCIADAS	
1.- Pruebas de funcionamiento. 2.- Determinación del daño que puede ser de hardware, software o conectividad. 3.- Daños de Hardware.- realizar pruebas de funcionamiento en caso de falla se deberá gestionar con el fabricante o vendedor el cambio del equipo o sus componentes. 4.- Daños de Software.- revisión de sistema operativo, bases de datos y aplicaciones, en caso de ser necesario se deberá restaurar backups y analizar dependencias de otros equipos o aplicaciones. 5.- Fallo en Redes.- revisar los enlaces de comunicaciones internos y externos, en caso de fallo gestionar con el proveedor la activación de los servicios, activar enlaces alternos. 6.- Si la solución del incidente ya sea de hardware, software o de redes requiere de un tiempo superior a 1 día se restituirá el servicio mediante un equipo provisional dentro o fuera de la institución.	
CONTINGENCIA	Enlaces Internet, Wan caídos
FUENTES DE RIESGO	**ESTIMACION DE RIESGO**
Infraestructura tecnológica Aplicaciones Instalaciones Equipos varios	Alto
RESPONSABLES	Oficial de seguridad informática, coordinador TI
ACCIONES ASOCIADAS	
1.-Herramienta de monitoreo de enlaces. 2.- Pruebas de conectividad a nivel local y externo, las pruebas deben incluir revisiones eléctricas de los equipos. 3.- Determinación del problema en equipos locales, remotos o enlace de comunicación. 4.- Contactar al proveedor del servicio e informar sobre el problema. 5.- Esperar respuesta del proveedor de acuerdo a los tiempos establecidos en los acuerdos de nivel de servicio y el contrato. 6.- Si se presenta un daño físico del equipo o sus componentes, el proveedor deberá reemplazarlo de manera inmediata. 7.- Si se produjeron daños en la configuración el proveedor deberá reconfigurar los equipos en los tiempos establecidos. 8.- Si el tiempo de respuesta se expande más de lo estimado se deberá activar el enlace de respaldo.	
CONTINGENCIA	Daño o mal funcionamiento en equipo de seguridad perimetral o switch core
FUENTES DE RIESGO	**ESTIMACION DE RIESGO**
Infraestructura tecnológica Aplicaciones Instalaciones Equipos varios	Alto
RESPONSABLES	Oficial de seguridad informática, coordinador TI, redes

ACCIONES ASOCIADAS	
1.- Herramienta de monitoreo de enlaces. 2.- Pruebas de conectividad de los equipos, las pruebas deben incluir revisiones eléctricas, físicas y configuraciones. 3.- Determinación del problema en el equipo (hardware y/o configuración). 4.- En caso de daño en la configuración se deberá restaurar el backup correspondiente. 5.- Si el daño es un componente del equipo se podrá reemplazarlo, en caso de no tenerlo se deberá solicitar al proveedor la venta del mismo. 6.- Analizar la posibilidad de reconfigurar el equipo para solventar el problema temporalmente. 7.- Si el daño del equipo es grave se deberá notificar al proveedor. 8.- En caso de tener que reemplazar el equipo, el proveedor deberá instalar un equipo provisional que solvente los requerimientos de la institución. 9.- Registro de eventos y soluciones aplicadas.	
CONTINGENCIA	Daño o corrupción de las bases de datos
FUENTES DE RIESGO	**ESTIMACION DE RIESGO**
Infraestructura tecnológica Aplicaciones	Alto
RESPONSABLES	Oficial de seguridad informática, coordinador TI, Aplicaciones
ACCIONES ASOCIADAS	
1.- Herramienta de monitoreo de aplicaciones. 2.- Pruebas de conectividad de los equipos, las pruebas deben incluir revisiones eléctricas, físicas y configuraciones. 3.- Determinación del problema en el equipo (hardware y/o configuración). 4.- Si el problema es de configuración se deben verificar los parámetros de configuración y ajustar el motor de bases de datos de acuerdo al procedimiento de recuperación y registrar una memoria técnica los errores y problemas corregidos, durante el evento. 5.- Si el daño está en el motor de las bases de datos, se deberá volver a instalarlo y restaurar la base de datos, esto en base al procedimiento de restauración de bases de datos. 6.- En caso de que la información se encuentre corrupta, se deberá ejecutar los procedimientos dentro de la base de datos para sanear la información.	
CONTINGENCIA	Daños equipos de escritorio usuario
FUENTES DE RIESGO	**ESTIMACION DE RIESGO**
Infraestructura tecnológica Aplicaciones Instalaciones Equipos varios	Alto
RESPONSABLES	Oficial de seguridad informática, coordinador TI, servicios TI
ACCIONES ASOCIADAS	

1.- Implementación herramienta de mesa de ayuda.
2.- Designación de caso a personal de soporte.
3.- Revisión y determinación del daño.
4.- Daños de Hardware.- realizar pruebas de funcionamiento en caso de falla se deberá gestionar la validación de garantía con el fabricante o vendedor para el cambio del equipo o sus componentes.
5.- Daños de Software.- revisión de sistema operativo y aplicaciones, en caso de ser necesario formatear realizar el respaldo de información.
5.- Fallo en Redes.- revisar el equipo de comunicación al cual se conecta, de ser necesario solicitar la revisión de la configuración del puerto.
6.- Validar credenciales y perfil dentro del directorio activo.

4.7.2 Plan de Respaldos.

El plan de respaldos de la información está enfocado a mantener los respaldos de la información y en el caso de necesitarlos estén disponibles para su restauración. EL respaldo de la información será definido y establecido en la política de respaldos la cual debe tomar en cuenta los siguientes parámetros:

- Información a respaldar
- Clasificar la información (critica, vital, etc.)
- Definir la periodicidad y tipo (completo, incremental, diferencial) de los respaldos
- Definir horarios de los respaldos
- Lugar de alojamiento de los respaldos
- Herramienta de gestión de respaldos
- Tiempo de almacenamiento de respaldos
- Pruebas de restauración donde se estimen tiempos.
- Responsable de los procesos de respaldos

- Registro y documentación de los respaldos y eventos presentados con la información.

4.7.3 Plan de Recuperación.

El plan de recuperación consiste en implementar mecanismos o procesos que ayuden a disminuir el impacto que ocasionaría un incidente y por lo tanto lo servicios y aplicaciones críticas de la institución se vean afectadas el menor tiempo posible. El plan de recuperación de desastre es el documento donde se deberá tomar en cuenta los siguientes aspectos:

- Identificar los eventos que denotan posibles desastres.
- Las personas en la institución que tienen la autoridad para declarar un desastre.
- La secuencia de eventos necesaria para preparar el sitio de respaldo una vez declarado el desastre.
- Las tareas y responsabilidades de todo el personal responsable para ejecutar el plan.
- Inventario del hardware necesario y del software requerido para restaurar las aplicaciones y servicios en la institución.
- Personal responsable para cubrir el sitio de respaldo.
- La secuencia de eventos necesaria para trasladar las operaciones desde el lugar de respaldo al sitio nuevo/provisional centro de datos.

- Documentar los cambios, eventos y acciones tomadas ante un incidente.

(Red Hat Inc., 2005)

De manera general, las instituciones que desarrollan el plan de recuperación deberán considerar los recursos a su alcance, los servicios previamente identificados y que se desean recuperar tan pronto como sea posible, así como los tipos y severidad de las amenazas que enfrenta la institución y que pueden llegar a convertirse en un problema de mayor magnitud para la misma. Otro elemento necesario es la proclividad al riesgo de la institución, ya que de ello también dependerán los esfuerzos y recursos destinados al desarrollo y aplicación del plan de recuperación. La consideración de este plan ofrece la ventaja de responder de forma planeada ante una catástrofe y minimizar su impacto en contra de los objetivos y misión de la institución de manera proactiva.

5 Análisis Costo-Beneficio

El análisis costo beneficio dentro de este plan de contingencia permitirá determinar que los costos de su implementación son justificables ante la presencia de desastres que tengan un impacto negativo en la institución.

5.1 Costos de Implementación

Se debe tener en cuenta que cuando los servicios y sistemas dejan de funcionar la institución puede tolerar un máximo de días sin que la información

perdida se vuelva imposible de recuperar y la institución empiece a asumir pérdidas tanto económicas como de imagen por la falta de información. Cabe aclarar que aun cuando la información pueda ser recuperada esto también implica costos de tiempo de trabajo de los funcionarios que deben cumplir horas extras para poder actualizar los sistemas y brindar servicios a la ciudadanía.

5.1.1 Costos Personal Técnico.

A continuación se proceden a considerar los costos referenciales para la implementación del plan de contingencia con respecto al personal técnico y funcionarios:

Tabla 38
Costo personal técnico BCP

Recurso	Involucrados	Cantidad	Precio	Costo
Capacitación en plan de contingencia de TI	Personal TIC	10	1000	10000
Capacitación en seguridad contra incendios	Personal Institución	50	0	0
Elaboración de plan de evacuación ante desastres naturales	Consultor	1	5000	5000
Capacitación primeros auxilios	Personal Institución	100	0	0
			total	15000

5.1.2 Costos Infraestructura.

A continuación se proceden a considerar los costos referenciales para la implementación de un centro de datos alterno que sirvan como equipos de

redundancia dentro del plan de contingencia con respecto a la infraestructura física y tecnológica:

Tabla 39
Costos infraestructura BCP

Recurso	Involucrados	Cantidad	Precio	Costo
Servidores	Personal TI	6	12000	72000
SAN	Personal TI	1	80000	80000
Switch core	Personal TI	1	40000	40000
Switch distribución	Personal TI	4	8000	32000
Firewall	Personal TI	1	16000	16000
Rack	Personal TI	1	1200	1200
Equipos de conexión	Personal TI	1	10000	10000
Equipo adicional		1	5000	5000
Enlaces de comunicación		1	5000	5000
Sistema contra incendios		1	3000	3000
Stock dispositivos para equipos pcs usuarios como discos duros, memorias, ups, etc.		1	10000	10000
			total	274200

5.1.3 Costos Aplicaciones y Herramientas.

A continuación se proceden a considerar los costos referenciales para la implementación del plan de contingencia con respecto a los sistemas y herramientas de monitoreo:

Tabla 40
Costos aplicaciones y software BCP

Recurso	Involucrados	Cantidad	Precio	Costo
Aplicación de monitoreo y control de incendios	Personal TI	1	8000	8000
Sistema de control de temperatura, humedad e inundaciones	Personal TI	1	5500	5500
Sistema de control de accesos al centro de datos	Personal TI	1	12000	12000
			total	25500

5.2 Justificación de Costos

La justificación de costos está enfocada a definir que es necesaria la inversión en infraestructura, aplicaciones y personal para evitar o reducir al mínimo el tiempo de inactividad de los servicios y aplicaciones que ocasionarían una pérdida económica y de imagen para la institución.

5.2.1 Análisis de los Costos

De acuerdo a los costos que involucran la implementación del plan de contingencia y en base a los recursos que posea la institución se realizara el análisis de costos. Es necesario realizar un análisis de los incidentes que se generan en un periodo de tiempo, en este caso será de un año, donde se tomaran los costos tanto en personal técnico, equipos tecnológicos, enlaces de comunicaciones así como del software utilizado para mitigar el impacto ocasionado por los incidentes presentados.

Tabla 41
Costos de pérdidas por daños equipos tecnológicos críticos

Problema	Costo	Descripción	Frecuencia	Costo Total
Daño servidores	12000	Servidores críticos de la institución (6)	1	72000
Daño firewall	16000	Equipo de seguridad perimetral	1	16000
Daño switch core	40000	Switch permite tráfico intervlan en la institución	1	40000
Daño switchs distribución, acceso	8000	Switch conectividad usuarios de la institución (4 áreas)	1	32000

Daño cableado estructurado	150	Cableado estructurado, centro de datos, áreas de la institución, (500 puntos aprox.)	1	75000
Perdida de respaldos bases de datos	10000	Información de los sistemas de la institución (suma de perdidas sistemas gestión penitenciaria y audiencias) por 360 días	1	3600000
Daño en storage	80000	Almacenamiento información	1	80000
Avería aire acondicionado	12000	Se deben bajar todos los servicios	1	12000
Daño UPS	30000	Se deben bajar todos los servicios	1	30000
Documentos, manuales, procesos	50000	Pago de honorarios de tres especialistas por un año	1	50000
Sistema de gestión penitenciaria	8000	Ingresos y egresos de PPLs[9] costo diario por PPL $10 (20 PPLs * 40 centros) esto por 360 días	1	0
Sistema de audiencias	2000	Traslado de PPLs Audiencias costo diario por PPL $5 (10 PPLs * 40 centros) esto por 360 días	1	0
			total	4007000

5.2.2 Beneficios.

Finalmente después de haber identificado los costos de implementación y mantenimiento para la ejecución del plan de contingencia se procede a realizar el cálculo de la relación costo - beneficio de la siguiente manera:

$$R_{b/c} = \frac{beneficios}{costos} = \frac{4007000}{314700} = 12{,}73$$

[9] PPLs.- Persona Privada de Libertad.

Como se puede observar el resultado de $R_{b/c}$ es mayor a uno, por lo tanto se indica que los beneficios superan los costos; por consiguiente la implementación del plan de contingencia debe ser considerado ya que beneficia a la institución y a la ciudadanía.

6 Definición de Procesos y Procedimientos

6.1 Documentación de los procesos identificados

Como se mencionó anteriormente es necesario contar con una serie de documentos que sirvan de insumo en la aplicación del plan de contingencia tanto en el inicio, durante y luego de presentarse el incidente o catástrofe. A continuación se procede a indicar los documentos necesarios que permitirán la implementación y ejecución del plan de contingencia:

Tabla 42
Documentación institución

No	Descripción	Identificador
1	Control de revisión y aprobación del documento	PLTC-01
2	Información áreas	PLTC-02
3	Inventario de Software y Hardware	PLTC-03
4	Tiempos de interrupción servicios	PLTC-04
5	Organización plan continuidad	PLTC-05
6	Establecimiento equipos contingencia	PLTC-06
7	Agenda contactos proveedores	PLTC-07
8	Sitio alterno respaldos	PLTC-08
9	Procedimiento recuperación equipos tecnológicos	PLTC-09
10	Procedimiento recuperación aplicaciones informáticas	PLTC-10
11	Procedimiento recuperación comunicaciones	PLTC-11
12	Registro estado de eventos	PLTC-12
13	Evaluación infraestructura tecnológica critica	PLTC-13

14	Perfiles de usuarios	PLTC-14

6.2 Procedimientos para ejecución de los procesos identificados

A continuación se presenta la hoja de ruta con los documentos incluidos dentro del plan de contingencia y registro de control para la revisión del plan de contingencia:

Tabla 43
Hoja de ruta documentación

HOJA DE RUTA DOCUMENTACION	Indicador	FECHA
Control de revisión y aprobación del documento	PLTC-01	
Información áreas	PLTC-02	
Inventario de Software y Hardware	PLTC-03	
Tiempos de interrupción servicios	PLTC-04	
Organización plan continuidad	PLTC-05	
Establecimiento equipos contingencia	PLTC-06	
Agenda contactos proveedores	PLTC-07	
Sitio alterno respaldos	PLTC-08	
Procedimiento recuperación equipos tecnológicos	PLTC-09	
Procedimiento recuperación aplicaciones informáticas	PLTC-10	
Procedimiento recuperación comunicaciones	PLTC-11	
Registro estado de eventos	PLTC-12	
Evaluación infraestructura tecnológica critica	PLTC-13	
Perfiles de usuarios	PLTC-14	

A continuación se procede a indicar el formulario de revisión y aprobación del documento.

Ministerio de Justicia, Derechos Humanos y Cultos	**Control de revisión y aprobación del documento**		Código: PLTC-01
			Versión:
			Fecha:
Historial de revisiones			
Versión	Autor	Fecha	Revisión

Control de revisiones			
	Responsable	Firma	Fecha
Control de pruebas			
	Responsable	Fecha	Resultados

A continuación se presenta el formulario donde se registra la información de las áreas de la institución, que en caso de presentarse un incidente servirán de apoyo en la aplicación del plan de contingencia:

Ministerio de Justicia, Derechos Humanos y Cultos	**Información del área**	Código: PLTC-02 Versión: Fecha:
Nombre de la unidad	RRSS	
Dirección	Av. Colon y reina victoria esq.	
Ciudad	Quito	
Teléfonos	22546608	
Unidad	Dirección Nacional de Rehabilitación Social	
Coordinador	Responsable de la unidad y encargado de gestionar los eventos de mitigación al ocurrir un incidente. Coordina actividades con el CPC	
Nombre contacto 1	Dra. Cristina Chamorro, Subsecretaria de RRSS	
Teléfonos	22546608 ext. 123	
Correo	acchamorro@minjusticia.gob.ec	
Unidad	Dirección Nacional de Rehabilitación Social	
Coordinador suplente	Encargado de apoyar las actividades del coordinador, y en caso de ausencia del mismo relevarlo en sus funciones	
Nombre contacto 2	Ab. Gustavo Terán, analista RRSS	

Teléfonos	22546608 ext. 124
Correo	gteran@minjusticia.gob.ec
Unidad	Dirección Nacional de Rehabilitación Social

A continuación se presenta el formulario del levantamiento y registro de los activos críticos de la institución:

Ministerio de Justicia, Derechos Humanos y Cultos	**Inventario de Equipos tecnológicos**					Código: PLTC-03 Fecha: Edición:		
Código activo	**Marca / modelo**	**Descripción**	**Fecha ingreso**	**Ubicación**	**Especificaciones técnicas**	**Estado**	**Custodio**	**Fecha mantenimiento**	**Servicios**
DNTIC-01192820-128	HP proliant dl360 g6	Servidor WEB linux, apache, mysql, php	10/09/2013	Centro de datos planta central	Memoria técnica proveedor	Operativo	Adrian Guayasamin	12/09/2015	Portal web institución

A continuación se presenta el formulario de registro de los tiempos máximos de interrupción de los servicios y aplicaciones de la institución:

Ministerio de Justicia, Derechos Humanos y Cultos	**Tiempos de interrupción servicios**					Código: PLTC-04 Versión: Fecha:	
Área/ Unidad	**Funciones afectadas**	**Sistema informático**	**Factor riesgo**	**TMI**	**TR**	**RPO**	**Criticidad**

Rehabilitación Social	Personas privadas libertad	esigpen	O,C	24h	6h	8h	5
	Adolecentes conflicto ley	casi	O,C	4h	5h	8h	4
	Planeación	poa	I,C	48h	2h	12h	4
	Video conferencia	real precense	C	24h	8h	8h	3
Coordinación administrativa -financiera	Garantías	grti	O	72h	6h	12h	3
	Finanzas	esigef	I,C	24h	8h	8h	4
	Compras públicas	esercop	C,O	24h	8h	8h	3
	Bienes	olympo	O	48h	6h	12h	3
	Contabilidad	cntb	I,C,O	24h	6h	8h	4
Talento Humano	Nomina	itthh	O	4h	4h	8h	4
	Control de asistencia	tasiste	O	72h	2h	12h	3
Atención Ciudadanía	Consultas ciudadanía	sirec	O	24h	6h	12h	3
Toda la institución	Mensajería	open fire	C	8h	6h	h	3
	Correo electrónico	Exchange	O,C,I	24h	8h	8h	4
	Gestión documental	Cobus	O,C,I	48h	8h	8h	3
	Portal web	Wordpress	O	24h	4h	8h	3
	Mesa de ayuda	Otrs	O	48h	6h	8h	3

Factores de riesgo sistemas informáticos:

- I: integridad
- O: operatividad
- C: confidencialidad
- TMI: tiempo máximo de interrupción
- TR: tiempo de recuperación
- RPO: tiempo de perdida de datos
- Criticidad: 5-máxima, 1-minima

A continuación se presenta el formulario donde se indica las diferentes funciones que realizará el personal de las áreas de TI involucradas en el las etapas de la implementación del plan de contingencia:

Redes y comunicaciones	Mantener y monitorear los enlaces de comunicación y redes
Redes y comunicaciones	Controlar la seguridad perimetral de la institución
Infraestructura	Supervisar y controlar el correcto funcionamiento de los equipos tecnológicos del centro de datos
Infraestructura	Mantenimiento y configuración de los equipos tecnológicos
Servicios	Soporte y mantenimiento de equipos de los funcionarios
Servicios	Configuración y asignación de permisos de acceso a servicios de la institución
Aplicaciones	Desarrollo y mantenimiento de aplicaciones
Aplicaciones	Responsables del almacenamiento y respaldos de la información
Aplicaciones	Responsable de los códigos fuentes
Aplicaciones	Asignación de permisos de acceso a usuarios de aplicaciones

A continuación se presenta el formulario con la información de las personas responsables de las áreas de TI en la institución para la implementación del plan de contingencia:

Ministerio de Justicia, Derechos Humanos y Cultos	**Establecimiento equipos contingencia**			Código: PLTC-06	
				Versión:	
				Fecha:	
Equipo	Nombre	Rol	Dirección	Teléfono 1	Teléfono 2
Recuperación sistema gestión penitenciaria	Adrian Guayasamin	Equipo aplicaciones	Sangolqui	2654234	986363636
	Luis Montenegro	Equipo Redes	Sur	2345678	983736763
	Maritza Onofa	Equipo Infraestructura	Sur	2345987	93838383

A continuación se presenta el formulario donde se realiza el registro de la información de los contactos externos (policía, cruz roja, proveedores de servicios, etc.) a la institución los mismos que prestaran sus servicios en caso de algún incidente que afecte la continuidad de los servicios:

Ministerio de Justicia, Derechos Humanos y Cultos	**Agenda contactos proveedores**		Código: PLTC-07
			Versión:
			Fecha:
Nombre	Compuhelp		
Descripción	Equipos tecnológicos, soporte y actualización		
Teléfonos	2233444 / 234324324 ext 2		
Dirección	Avenida Eloy Alfaro y amazonas		
Correo	soporte@compuhelp.cpm		
Contactos			
Nombre	correo	teléfonos	cargo
Juan Carlos Inga	jcinga@compuhelp.com	23937833 / 093837474	especialista servidores, san
Byron Arroyo	barroyo@compuhelp.com	23937833 / 09836354242	gerente de servicios

A continuación se presenta el formulario con información de los lugares donde se almacenan los respaldos de la información de la institución:

Ministerio de Justicia, Derechos Humanos y Cultos	**Sitio alterno respaldos**	Código: PLTC-08
		Versión:
		Fecha:

Información del Sitio	
Sitio	SNAP
Dirección	Av. Colón y 9 de octubre edificio paco
Teléfonos	233344 / 233333 ext. 23
Contactos	María Isabel Tejada, mitejada@snap.gob.ec

Información del respaldo							
Descripción	Código	Tipo respaldo	Periodicidad	Medio almacenamiento	Responsable	Fecha / hora	Nro. Copias
Sistema de gestión penitenciaria	esigpen-2015-01-01	Completo	Diario	Cintas	Adrián Guayasamin	12-01-2015-1200	2
Sistema de control de asistencia	tasiste-2015-01-01	Completo	Diario	Cintas, DVD.	Maritza Onofa	12-01-2015-1200	3

A continuación se presenta el formulario para el registro de los procedimientos de recuperación de equipos tecnológicos críticos de la institución:

Ministerio de Justicia, Derechos Humanos y Cultos	**Procedimiento recuperación equipos tecnológicos**	Código: PLTC-09
		Versión:
		Fecha:
Equipo	Sistema de Gestión Penitenciaria	
Objetivo	Registrar la información necesaria para reanudar el funcionamiento del sistema de gestión penitenciaria del Ministerio de Justicia, Derechos Humanos y Cultos	
Responsables	Adrián Guayasamin, coordinador aplicaciones Maritza Onofa, coordinadora de infraestructura Luis Montenegro, coordinador de redes y comunicaciones	
Integrantes equipos de recuperación		
Coordinador del equipo		
Principal	Hector Santander	
Suplente	Fernando Tirado	
Integrantes del equipo		
Integrante	Adrián Guayasamin, coordinador aplicaciones	
Integrante	Maritza Onofa, coordinadora de infraestructura	
Integrante	Luis Montenegro, coordinador de redes y comunicaciones	
Integrante		
Integrante		
Características del equipo		
Marca	HP	
Modelo	Proliant DL360 G6	
Almacenamiento	sata 2 hdd 500gb	
	RAID (Serial ATA-150 / SAS) - PCI Express x8 (Smart Array P410i)	
	hotswap	
Memoria	32 gb ram	
	DDR3 SDRAM - 1333 MHz - PC3-10600	
Red	Adaptador de red - Ethernet, Fast Ethernet, Gigabit Ethernet - Puertos Ethernet : 4 x Gigabit Ethernet	
Alimentación	4 fuentes de poder hotswap	
	CA 120/230 V (50/60 Hz)	
Procesador	2 Quad-Core Xeon E5520 / 2.26 GHz (Quad-Core)	
Garantía	3 años de garantía	
	hasta diciembre 2016	

Mantenimiento	vigente	
	2 veces por año	
Recuperación del equipo		
Acciones necesarias requeridas en el proceso de recuperación.		
Acción	Procedimiento	Tiempo
Instalación Sistema Operativo	Instalación de centos 6, versión gui	30 min
Configuración red	etho ip:192.168.10.24 msc:255.255.255.0 gw:192.168.10.1 eth1 ip:192.168.60.24 msc:255.255.255.0 gw:192.168.60.1 dns1:192.168.10.24 dns2: 192.168.5.24	10 min
Creación de usuarios	usuario con privilegios de administrador	5 min
Asignación de nombre de equipo	17uioMjdhcEsigpen01	2 min
Actualización del Sistema Operativo	Actualización de repositorios del SO	20 min
Configuración Firewall	Activación y configuración iptables, clinux	10 min
Pruebas de conectividad	test de conexión con firewall institución test de conexión directorio activo test de conexión servidor dns test de conexión servidor base de datos	10 min
Contactos externos		
Contactos requeridos como proveedores, equipo técnico		
Institución	Nombre	Teléfonos
Compuhelp	Juan Carlos Inga	9873746474
CNT	Henry Mayorga	253373873

A continuación se presenta el formulario para la recuperación de software y/o aplicaciones de la institución en caso de un incidente:

Ministerio de Justicia, Derechos Humanos y Cultos	**Procedimiento recuperación aplicaciones informáticas**	Código: PLTC-10 Versión: Fecha:
Aplicación	Esigpen	
Objetivo	Registrar la información necesaria para reanudar el funcionamiento del sistema de gestión penitenciaria del Ministerio de Justicia, Derechos Humanos y Cultos	
Responsables	Adrian Guayasamin, coordinador aplicaciones Maritza Onofa, coordinadora de infraestructura Luis Montenegro, coordinador de redes y comunicaciones	
Integrantes equipos de recuperación		
Coordinador del equipo		
Principal	Diego Pozo	
Suplente	Maria Jose Espinoza	
Integrantes del equipo		
Integrante	Adrian Guayasamin, coordinador aplicaciones	
Integrante	Maritza Onofa, coordinadora de infraestructura	
Integrante	Luis Montenegro, coordinador de redes y comunicaciones	
Integrante		
Integrante		
Información de la Aplicación		
Versión	Versión 2.0	
Sistema Operativo	Linux centos 6	
Dependencias	Servidor de base de datos Servidor de logs Firewall	
Aplicación	Software de código abierto java	
	Base de datos postgres	
	Contenedor web de aplicación tomcat	
	Desarrollo personal TI de la institución	
Recuperación de la aplicación		
Recursos requeridos previo y durante el proceso de recuperación		
Acción	Procedimiento	Tiempo
Respaldo	Traslado del respaldo al sitio	30 min
Instalación Java	Instalar version 1.7 de java yum -y install java	20 min
Instalación Tomcat	Instalar versión 7 de apache tomcat: descargar tomcat tar -xzf jdk-7u5-linux-x64.tar.gz	30 min
Instalación Postgres	Instalación de postgres yum install postgresql-server	20 min

Configuración java	Realizar el seteo de las variables del sistema: whereis java vim /etc/profile export JAVA_HOME=/usr/lib/jvm/jre-1.6.0-openjdk.x86_64 export PATH=$PATH:/usr/lib/jvm/jre-1.6.0-openjdk.x86_64/bin	5 min
Configuración postgres	Configurar y crear base de datos postgres: service postgresql-9.4 initdb service postgresql-9.4 start chkconfig postgresql-9.4 on systemctl enable postgresql-9.4 systemctl start postgresql-9.4 su – postgres	10 min
Restaurar base de datos	Resturar respaldo de la base de datos: # psql -U usuario -d mjdhc -p 5432 -h 192.168.10.24 < esigpen-01-01-2015.sql	30 min
Restaurar aplicación	Restaurar respaldo de la aplicación. War	10 min
Configuración servicios	Configurar servicios y demonios de tomcat: service tomcat restart	20 min
Configurar tareas	Configurar tareas de respaldos base de datos	10 min
Pruebas	Realizar pruebas internas y externas de acceso	5 min
Producción	Subir a producción la aplicación	2 min
Contactos externos		
Contactos requeridos como proveedores, equipo técnico		
Institución	Nombre	Teléfonos

A continuación se presenta el formulario para la recuperación de las comunicaciones de la institución en caso de un incidente:

Ministerio de Justicia, Derechos Humanos y Cultos	**Procedimiento recuperación de las Comunicaciones**	Código: PLTC-11 Versión: Fecha:
Equipo	Switch de core	
Objetivo	Registrar la información necesaria para reanudar el funcionamiento del equipo de comunicaciones switch de core del Ministerio de Justicia, Derechos Humanos y Cultos	
Responsables	Maritza Onofa, coordinadora de infraestructura Luis Montenegro, coordinador de redes y comunicaciones	

Integrantes equipos de recuperación		
Coordinador del equipo		
Principal	Roberto Vaca	
Suplente	Pamela Zumarraga	
Integrantes del equipo		
Integrante	Maritza Onofa, coordinadora de infraestructura	
Integrante	Luis Montenegro, coordinador de redes y comunicaciones	
Integrante		
Integrante		
Integrante		
Información del equipo		
Marca	HP	
Modelo	HP Switch 5406zl (J8697A)	
Usuario	admin	
Clave	XXXXX	
Dirección IP	192.168.5.9	
Mac address	08 2e 5f 3b e5 00	
Número serie	SG19DXT3C0	
Versión	K.15.16.0008, ROM K.15.30	
Almacenamiento		
Memoria		
Red		
Alimentación		
Procesador		
Garantía	3 años de garantía	
	hasta diciembre 2016	
Mantenimiento	vigente	
	2 veces por año	
Recuperación del Equipo		
Recursos requeridos previo y durante el proceso de recuperación		
Acción	Procedimiento	Tiempo
Respaldo	Traslado del respaldo al sitio	30 min
Validar equipo	Proceso de validación del equipo	10 min
Garantía equipo	Validar garantía, reemplazo partes o equipo proveedor	6 horas
Reseteo equipo	Realizar reseteo a valores de fabrica	20 min
Restaurar respaldo	Realizar restauración del archivo de configuración	10 min
Pruebas	Realizar pruebas internas y externas de acceso	5 min
Producción	Subir a producción la aplicación	2 min
Contactos externos		
Contactos requeridos como proveedores, equipo técnico		

Institución	Nombre	Teléfonos
Compuhelp	Juan Carlos Inga	093287334
Point technical	Edwin Gualichico	098363633

A continuación se presenta el formulario donde se registra los eventos o incidentes suscitados, así como las actividades realizadas durante la aplicación del plan de contingencia.

Ministerio de Justicia, Derechos Humanos y Cultos	**Registro estado de eventos**		Código: PLTC-12 Versión: Fecha:
Incidente	No hay acceso a servidor base de datos		
Lugar	Planta Central		
Reporta	XXXXXXXX usuario base de datos		
Responsable	Adrian Guayasamin, coordinador de aplicaciones Luis Montenegro, coordinador de redes y comunicaciones		
Seguimiento			
Actividad	Procedimiento aplicado	Resultado	Fecha
Verificar Equipos físico		correcto	
Verificar aplicaciones		correcto	
Verificar conectividad física		fallo	
Pruebas de conectividad		fallo	
Verificación equipo comunicaciones		fallo	

A continuación se procede a mostrar el formulario que permite evaluar la infraestructura tecnológica crítica de la institución luego de presentarse un incidente o catástrofe:

Ministerio de Justicia, Derechos Humanos y Cultos	**Evaluación infraestructura tecnológica critica**		Código: PLTC-13
			Versión:
			Fecha:
Incidente	Temblor		
Lugar	Centro de datos		
Responsable	Director TI		
Evaluación			
Equipo	Condición	Tiempo recuperación	Observaciones
Servidor correo	Dañado, puede seguir trabajando	Validar garantía, 4 horas	Cambiar fuente poder
Servidor aplicaciones	Dañado leve, corregir para trabajar	2 horas	
Servidor base datos	Sin daños	X	X
Equipos de comunicaciones	Sin daños	X	X
Condición	Sin daños		
	Dañado, puede seguir trabajando		
	Dañado leve, corregir para trabajar		
	Dañado grave, reparar para trabajar		

A continuación se procede a indicar el formulario donde se registra el perfil de los usuarios que son los responsables o encargados de manejar las

aplicaciones críticas de la institución, donde es necesario configurar o personalizar las aplicaciones para su respectivo funcionamiento:

Ministerio de Justicia, Derechos Humanos y Cultos	**Perfiles de Usuarios-Equipos**	Código: PLTC-14
		Versión:
		Fecha:
Cargo: Director Nacional de Rehabilitación Social		
Nombre: Gustavo Peñafiel		
Usuario: peñafielg		
Área: Rehabilitación Social		
Aplicaciones Generales instaladas		
Open Office, adobe reader		
Mozilla Firefox, google chrome, flash player		
Antivirus		
Aplicaciones Adicionales instaladas		
Java		
Qlikview desktop		
Acceso Aplicaciones Institucionales		
Correo electrónico		
Sistema de Gestión Penitenciaria esigpen		
Tableros reportes qlikview		
Sistema de Visitas		
Configuración Red		
Direccionamiento: dinámico		
ip:		
Mascara:		
Gateway:		
Dns:		
Vlan:		
Dhcp server:		
Información Equipo		
Área: Rehabilitación Social		
Ubicación: Mezanine		
Nombre equipo: MJDHC-RRSS-17uio0xxx		

Dominio: int.minjusticia.gob.ec
Custodio: Gustavo Peñafiel
Equipos Asociados
Impresora red rrss
Observaciones

7 Conclusiones y recomendaciones

Finalmente como resultado final del desarrollo del proyecto de tesis “ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA SISTEMAS INFORMÁTICOS – CASO DE ESTUDIO MINISTERIO DE JUSTICIA, DERECHOS HUMANOS Y CULTOS” se procede a emitir las siguientes conclusiones y recomendaciones las mismas que permitirán resumir de mejor manera el proyecto y mejorar ciertos criterios y planteamientos sobre el mismo.

7.1 Conclusiones

- La evaluación de los riesgos de TIC que afectan a la continuidad del negocio es un proceso sumamente importante ya que permitirá determinar las falencias tecnológicas que posee la institución, las mismas que servirán como insumo para la elaboración del plan de contingencia.

- La evaluación y análisis de los riesgos de TIC sirve como base para la planificación e implementación del sistema de gestión de seguridad de la información, que parte de la determinación de los activos críticos de la institución , determinar las amenazas y vulnerabilidades a las que están expuestos las cuales serán gestionados con controles y procesos debidamente establecidos y probados.
- La gestión de riesgos que inciden en la generación de eventos críticos consiste en tratar de minimizar el impacto, así como de reducir el nivel de incidencia de estos sobre las operaciones de la institución.
- La gestión de riesgos conlleva un proceso de estudio, retroalimentación y coordinación entre las diferentes áreas de la institución involucradas en el proceso de aplicación de medidas preventivas y correctivas para reducir el impacto causado por la inactividad de las operaciones críticas de la institución.
- Las métricas de punto de recuperación y tiempo de recuperación permiten definir el tiempo necesario para que las operaciones se reanuden.
- Es necesario realizar el análisis donde se defina el tiempo estimado para reanudar las operaciones, del resultado del análisis se obtiene que para reducir el tiempo de reanudación de las operaciones es necesario implementar o contar con más

recursos tecnológicos y humanos; y esto a su vez involucra una mayor inversión económica.

- La continuidad del negocio de las TIC dependerá del plan de contingencia donde se establecen las acciones a realizar en momentos de emergencia; su implementación se realizará mediante la aplicación de políticas, procesos y procedimientos por parte de los responsables de las áreas involucradas de la institución.
- Los procesos, políticas y procedimientos para mantener la continuidad deben estar en constante revisión y actualización permitiendo de esta forma ser más eficientes y efectivos en caso de un incidente o evento.
- Es fundamental que el plan de contingencia sea aprobado por la máxima autoridad de la institución, y sea socializado a cada una de las áreas involucradas para su implementación.
- Es necesario que dentro del orgánico funcional de la institución se defina al personal responsable y sus colaboradores de cada una de las áreas donde se definan los cargos y roles necesarios para la implementación y mantención del plan de contingencia.
- Se debe concientizar a los funcionarios de la institución sobre el correcto uso de la infraestructura tecnológica y sobre todo de la seguridad de la información; para lo cual se aplicaran políticas, reglamentos y normativas donde se defina la obligatoriedad del correcto uso de los bienes de la institución.

7.2 Recomendaciones

- Se recomienda establecer un cronograma de evaluación de riesgos dentro del plan estratégico informático con el fin de mantener una constante verificación y control de riesgos.
- El personal encargado de la evaluación de riesgos debe estar debidamente capacitado y entrenado, y en caso de no ser así se buscara al personal idóneo para esta actividad.
- Tomar como referencia las lecciones aprendidas de la propia institución así como de entidades externas donde sus experiencias sirvan de guía para ser aplicadas en ciertos eventos o incidentes ocurridos en la institución.
- La institución debe solicitar el presupuesto para montar o contratar un centro de datos alterno donde se alberguen las aplicaciones críticas de la institución.
- Validar la vigencia de soporte y carepacks de la infraestructura tecnológica de la institución; de ser necesario se deberá presupuestar estos costos en el plan operativo anual de TIC en la institución.
- El levantamiento de los procesos, elaboración de políticas y procedimientos debe ser registrado o documentado utilizando herramientas tecnológicas que permitan estructurar, validar

control de cambios y almacenar la información de manera segura.

- Realizar campañas y talleres de prevención de desastres para todos los funcionarios de la institución.
- Establecer un cronograma de simulacros de desastres y coordinar con cada una de las áreas de la institución sus deberes y responsabilidades.
- Evaluar resultados de los simulacros y rediseñar tareas si así lo amerita.

Referencia Bibliográfica

Alegsa, L. (12 de 05 de 2010). *Definición de Tolerancia de fallas*. Obtenido de http://www.alegsa.com.ar/Dic/tolerancia%20de%20fallas.php

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (01 de 10 de 2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método.* Madrid, España: Ministerio de Hacienda y Administraciones Públicas Centro de Publicaciones. Obtenido de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VrJDiuZF3Ug

Amutio Gómez, M., Candau, J., & Mañas, J. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos.* Madrid: Ministerio de Hacienda y Administraciones Públicas Centro de Publicaciones.

Amutio Gómez, M., Candau, J., & Mañas, J. (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas.* Madrid, España: Ministerio de Hacienda y Administraciones Públicas Centro de Publicaciones. Obtenido de http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf

Chavez, R. (25 de 09 de 2013). *Gestión del Riesgos de Seguridad de la Información.* Obtenido de http://es.slideshare.net/roberth.chavez/gestin-del-riesgos-de-seguridad-de-la-informacin

contabilidad.com.py. (08 de 06 de 2006). *COSTOS DIRECTOS E INDIRECTOS*. Obtenido de

http://www.contabilidad.com.py/articulos_73_costos-directos-e-indirectos.html

Cruz, R. (18 de 08 de 2015). *Recuperación de desastres informáticos: Diseñe deseando lo mejor, en función de esperar lo peor*. Obtenido de http://blogs.vmware.com/latam/2015/08/recuperacion-de-desastres-informaticos-disene-deseando-lo-mejor-en-funcion-de-esperar-lo-peor.html

Eterovic, J. E., & Pagliari , G. (15 de 01 de 2011). *Metodología de Análisis de Riesgos Informáticos*. Obtenido de http://www.cyta.com.ar/ta1001/v10n1a3.htm

Gorenberg, A. (01 de 08 de 2006). *Comunicaciones de alta disponibilidad*. Obtenido de http://www.emb.cl/electroindustria/articulo.mvc?xid=544&edi=8

Horngren, C., Datar, S., & Rajan, M. (2012). *Contabilidad de costos. Un enfoque gerencial*. Obtenido de http://www.academia.edu/9740927/Contabilidad_de_costos._Un_enfoque_gerencial

Karman, V. (01 de 03 de 2004). *RPO y RTO*. Obtenido de http://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo

L. X. (15 de 03 de 2009). *ARQUITECTURA DE RED*. Obtenido de http://laurapita.blogspot.com/2009/03/arquitectura-de-red.html

MADEJA. (01 de 01 de 2013). *Conceptos sobre la escalabilidad*. Obtenido de http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/220

Marcos, G. (03 de 04 de 2011). *Redundancia, Contingencia, Continuidad, Resiliencia*. Obtenido de http://www.compuchannel.net/2011/04/03/redundancia-contingencia-continuidad-resiliencia/

Marcos, G. (22 de 03 de 2011). *Redundancia, Contingencia, Continuidad, Resiliencia* . Obtenido de http://www.notingenio.com/index.php?option=com_content&view=artic

le&id=729:redundancia-contingencia-continuidad-resiliencia&catid=44:columnista&Itemid=63

Moliner López, F. J. (01 de 08 de 2005). *Informáticos de la Generalitat Valenciana*. Obtenido de https://books.google.com.ec/books?id=Xy0AKwYMRqcC&pg=PA195&lpg=PA195&dq=est%C3%A1+directamente+relacionada+con+la+generalizaci%C3%B3n+del+uso+de+las+tecnolog%C3%ADas+de+la+informaci%C3%B3n,&source=bl&ots=9davH4qRHw&sig=X3POMY55j-QfuvfwMvUrMDEAIaY&hl=es&sa

Ortega, D. (13 de 01 de 2011). *Calidad en las TIC*. Obtenido de http://calidadtic.blogspot.com/2011/01/como-hacer-un-plan-de-contingencia.html

Osmer. (02 de 02 de 2013). *Beneficios Tangibles e Intangibles*.

Ramirez, L. (01 de 01 de 2016). *COMP TOL A FALLOS*. Obtenido de http://www.academia.edu/7004400/COMP_TOL_A_FALLOS

Red Hat Inc. (2005). *Introducción a la administración de sistemas.* USA: rhel-isa(ES)-4-Print-RHI.

Revista ALIDE. (01 de 03 de 2013). *¿Cómo gestionar activos de información?*

revista datacenter. (12 de 12 de 2013). *¿RTO vs RPO?* Obtenido de https://revistadatacenter.wordpress.com/2013/12/12/cual-es-la-diferencia-entre-el-rto-y-rpo/

Rodríguez Sánchez, Y. (30 de 11 de 2012). *Sistemas de Información en las Organizaciones.* Obtenido de http://www.ecured.cu/Sistemas_de_informaci%C3%B3n_en_las_organizaciones

Sánchez, N. (01 de 03 de 2013). *Plan de recuperación ante desastres (DRP)*. Obtenido de http://blog.celingest.com/2013/03/01/recuperacion-desastres-disaster-recovery/